FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS

"Modelo de Seguridad para el Control del Tráfico de la Red LAN, basado en la ISO/IEC 27002:2013 en Grupo SUEZ"

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

AUTOR:
Janter Edison Salazar Mateo

ASESOR:
Dr. Ing. Manuel Hilario Falcón

LÍNEA DE INVESTIGACIÓN:

Tecnologías de Información
Infraestructura y servicios de redes y comunicaciones

LIMA – PERÚ

2018

UCV UNIVERSIDAD CÉSAR VALLEJO	ACTA DE APROBACIÓN DE LA TESIS	Código : F07-PP-PR-02.02 Versión : 09 Fecha : 23-03-2018 Página : 1 de 1

El Jurado encargado de evaluar la tesis presentada por don (a): **JANTER EDISON SALAZAR MATEO** cuyo título es:

"MODELO DE SEGURIDAD PARA EL CONTROL DEL TRÁFICO DE LA RED LAN, BASADO EN LA ISO/IEC 27002:2013 EN GRUPO SUEZ"

Reunido en la fecha, escuchó la sustentación y la resolución de preguntas por el estudiante, otorgándole el calificativo de: 14(número) CATORCE (letras).

Lima, San Juan de Lurigancho 07 de diciembre del 2018

PRESIDENTE

SECRETARIO

VOCAL

Elaboró	Dirección de Investigación	Revisó	Responsable del SGC	Aprobó	Vicerrectorado de Investigación

Dedicatoria

Dedico de manera especial a mi madre Antonia Mateo H. pues ella fue el principal cimiento para la construcción de mi vida profesional, sentó en mis las bases de responsabilidad y ganas de superación, en ella tengo el espejo en el cual me quiero reflejar pues sus virtudes y su gran amor hacia mí me lleva admirarla cada día más.
Gracias Dios mío por concederme la mejor madre.

A mi padre Cerilo Salazar, mis hermanos y mis sobrinas que son las personas que me han ofrecido el amor y la calidez de familia a la cual amo.

Agradecimiento

En primer lugar, agradezco a mis docentes y asesores, personas de gran conocimiento quienes se han esforzado por ayudarme a llegar al punto en el que me encuentro.
Sencillo no ha sido el proceso, pero gracias a su voluntad de transmitirme sus sapiencias y dedicación que los ha regido, he logrado importantes objetivos como culminar el desarrollo de mi tesis con éxito y obtener una afable titulación profesional.

Declaración de Autenticidad

Yo, Janter Edison Salazar Mateo con DNI 42545103 a efecto de cumplir con las disposiciones vigentes consideradas en el reglamento de grados y títulos de la Universidad César Vallejo, facultad de ingeniería, escuela profesional de ingeniería de sistemas, declaro bajo juramento que toda la documentación que acompaño es original. Así mismo, declaro bajo juramento que todos los datos e información que se señala en la presente tesis son auténticos y veraces. En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada por lo cual me someto a lo dispuesto en las normas académicas de la Universidad Cesar Vallejo.

Lima, 30 de noviembre de 2018

Janter Edison Salazar Mateo
DNI. 42545103

Presentación

Señores miembros del jurado:

En cumplimiento del reglamento de grados y títulos de la Universidad César Vallejo presento ante ustedes la tesis titulada "modelo de seguridad para el control del tráfico de la red LAN, basado en la ISO/IEC 27002:2013 en grupo SUEZ", que comprende los capítulos instrucción, metodología, resultados, discusión, conclusiones y recomendaciones. El objetivo de la tesis fue determinar el efecto del modelo de seguridad y el control del tráfico en la red LAN, basado en la ISO/IEC 27002:2013 en Grupo SUEZ.
La misma que someto a vuestra consideración y espero que cumpla con los requisitos de aprobación para obtener el título profesional de ingeniero de sistemas.

Atte,

Janter Edison Salazar Mateo

Índice

Índice de Figuras

Índice de Tablas

Resumen

En esta investigación se ha desarrollado un modelo de seguridad perimetral lógico que controle al acceso a internet, y permita gestionar los roles de acceso de los usuarios finales del Grupo SUEZ. Es decir, se trata de un servidor proxy desarrollado en Linux Centos que se implementara en la red LAN y que gestionara los permisos de acceso para navegar en internet, de esta manera se lograra mayor eficiencia del ancho de banda de la red para un mejor uso del sistema de CONCAR (sistema de contabilidad) y STARSOFT (sistema de planillas) aplicativos internos que hace uso los colaboradores. El presente modelo de seguridad propuesto en la tesis es utilizado por su mayor uso y bajo costo en pymes y grandes compañías peruanas.

Palabras Clave: Linux, Centos , servidor proxy, seguridad perimetral.

Abstract

In this research, a logical perimetric security model has been developed that controls access to the internet, and allows managing the access roles of the final users of the SUEZ Group. That is to say, it is a proxy server developed in Linux Centos that will be implemented in the LAN network and that will manage the access permissions to surf the Internet, in this way greater efficiency of the network bandwidth will be achieved for a better use of the CONCAR system (accounting system) and STARSOFT (system of spreadsheets) internal applications that employees use. The present security model proposed in the thesis is used for its greater use and low cost in SMEs and large Peruvian companies.

Keywords: Linux, Centos, proxy server, perimeter security.

I. INTRODUCCION

1.1 Realidad Problemática

En Suiza, Israel, Finlandia, Suecia, Suecia y EEUU existen compañías privadas que cuentan con grandes sistemas de comunicaciones y redes que soportan el flujo de datos e información entre las computadoras y servidores. Asimismo, las compañías tienen claro en proteger de los ataques, virus y hackers la información es por eso que diversas organizaciones han implementado en sus redes sistemas de protección intrusos alineados a reglas de la seguridad para prevenir el robo de los datos, estas compañías consideran que la información y las personas son elementos muy importantes para la continuidad de los procesos del negocio. Desde la aparición del internet las empresas han tenido en cuenta los sistemas de seguridad en sus redes desde los antivirus personales hasta sistemas de seguridad perimetral en hardware como los Appliance que integran firewall, web filter, e-mail filter, proxy y VPN esto en un empaquetado que ha sido desarrollados su propio sistema operativo, en esta investigación se desarrollara un modelo de seguridad en Linux Centos. Las compañías a nivel mundial utilizan expertos sistemas de seguridad en todas las zonas de sus redes de información. Tales son como las compañías Microsoft, Google, Amazon y Facebook con sede en Estados Unidos, California. El reporte muestra países mejorando la capacidad de innovar sin dejar de lado la seguridad en sus redes de información.

Figura 1: Países con Tecnologías de la Información Avanzado

ECONOMIA/PAIS	2016	2015	VARIACION
Singapur	1	1	
Finlandia	2	2	
Suecia	3	3	
Noruega	4	5	
Estados Unidos	5	7	
Holanda	6	4	
Suiza	7	6	
Reino Unido	8	8	
Luxemburgo	9	9	
Japón	10	10	

Fuente[1]: The Global Information Technology WEF

En entrevista con Wendel Odom representante de Cisco señalo, que los empleados de todo el mundo manipulan las redes comerciales para notificar, ayudar entre sí y acceder a información. Las compañías ávidas de incrementar su producción buscan formar cada vez más las comunicaciones de red con las operaciones comerciales, e estimulan a que sus trabajadores

[1] The Global Information Techn

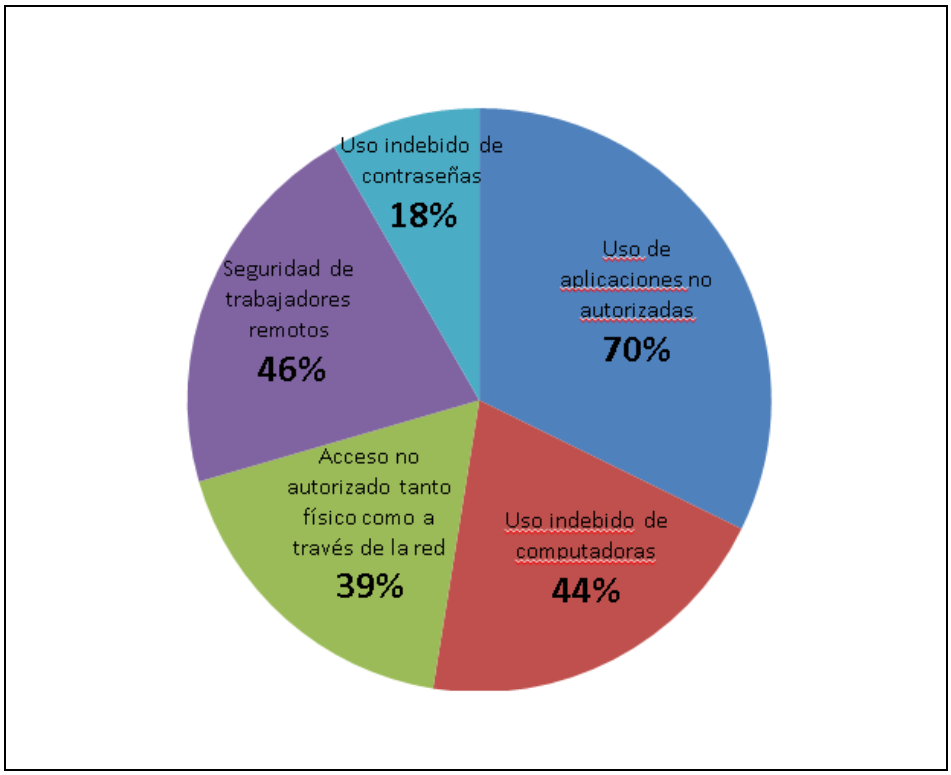
ology Report 2016 “World Economic Forum”.

aprovechen tecnologías tales como dispositivos inalámbricos y puntos de acceso públicos. La producción aumenta, pero la seguridad y colaboración basada en la red coloca la información empresarial en un entorno más amplio que es más vulnerable y difícil de proteger.

Figura 2: Costo en pérdidas por ataques cibernéticos en Perú

Fuente: Diario Gestión, Agosto 2017

Figura 3: Practicas Incorrectas de Empleados en el Grupo SUEZ



Fuente: Informe Técnico Cisco 2017

Tabla 1 : Practicas inadecuadas de empleados

- **Uso de aplicaciones no autorizadas:** el 70% de los técnicos de TI cree que el uso de Aplicaciones no autorizados fue responsable de hasta la mitad de los incidentes de pérdida de Información en sus compañias.
- **Uso indebido de PC de la compañia:** el 44% de los empleados comparte Aparatos de trabajo con otras personas sin supervisión.
- **Acceso no autorizado tanto físico como a través de la red:** el 39% de los técnicos de TI afirmó que ha debido abordar el acceso no autorizado por parte de un trabajador a zonas de la red o de las instalaciones de la empresa.

Fuente[2]: The Global Information Technology WEF

Tabla 2: Casos de inseguridad tecnológicas en otros países

- China muestra tal nivel de abuso tecnológico que los encargados de tomar decisiones de TI auditan las computadoras en busca de información no autorizada.
- En Japón, el 65% de los consumidores finales no acata de manera constante las reglas de TI de su compañía, y el estudio indica que el abuso tecnológico por parte de los trabajadores finales está en aumento.
- Los trabajadores finales en India tienden a emplear el e-amil y la mensajería instantánea para fines personales y modifican la configuración de seguridad de TI en las Pc's para poder ver paginas no autorizados.
- Los empleados en Brasil manejan las Pc's para fines de comunicación personal y para tareas como descargar videos.
- Los trabajadores de Francia tienen la tasa mínima de cumplimiento de reglas de TI de todos los países encuestados, ya que sólo el 16% de los trabajadores afirmó cumplir de manera constante las reglas de la empresa.

Fuente[3]: The Global Information Technology WEF

En américa Latina los países como Chile con 38%, Uruguay con 43%, Costa Rica con 44%, Panamá con 55%, Colombia con 68%, Paraguay con 105%, Venezuela con 108 % y Bolivia con 111%. Brasil con 72% es el país que está dando la importancia al uso de las tecnologías en los procesos de los negocio. Brasil es consiente que la tecnología avanza día a día y los ataques a la seguridad desde redes externos de malware y hackers también avanzan a pasos largos, por tanto en esa línea de acción la seguridad en las compañías brasileñas tiene que continuar cubriendo cada zona de las redes de una organización con el propósito proteger el robo de información y ser entregado a la competencia para el cobro de un rescate económico por la información.

[2] The Global Information Technology Report 2016 "World Economic Forum" (Innovating in the Digital Economy)
[3] The Global Information Technology Report 2016 "World Economic Forum" (Innovating in the Digital Economy)

Figura 4: Ranking de Paises Latinoamericanos con Tecnología de Información Avanzada

ECONOMIA/PAIS	2016	2015	VARIACION
Chile	38	38	
Uruguay	43	46	
Costa Rica	44	49	
Panamá	55	51	
Colombia	68	64	
Brasil	72	84	
México	76	69	
Argentina	89	91	
Perú	90	90	
El Salvador	93	80	
República Dominicana	98	95	
Paraguay	105	105	
Venezuela	108	103	
Bolivia	111	111	
Nicaragua	131	128	
Haiti	137	137	

Fuente[4]: The Global Information Technology WEF

(Trend Micro, Seguridad Cibernetica en America Latina, 2015) Estamos viviendo actualmente una etapa decisiva en materia de seguridad cibernética. Las noticias sobre incidentes cibernéticos de gran tamaño llenan los reportes diarios y se están convirtiendo cada vez más en objeto de deliberaciones políticas. Nuestro mayor temor de los ataques cibernéticos en las empresas latinoamericanas es que paralicen la infraestructura de los servicios que usa la población y generen caos como consecuencia una depresión económica. El internet es un bien compartido, y la seguridad cibernética es una responsabilidad compartida, lo que significa que es necesario que los empleados adquieran un sentido de propiedad y pongan en práctica buenos hábitos de seguridad en línea. La dependencia de las tecnologías de la información y las comunicaciones seguramente seguirá creciendo incesantemente. Por lo tanto, es necesario que los gobiernos y los dueños de las compañías adopten las medidas pertinentes para proteger y asegurar sus infraestructuras críticas iniciando o promoviendo continuamente planes y legislación sobre seguridad cibernética, aumentando la cooperación internacional y obteniendo la participación de todas las partes interesadas.

Una prestigiosa compañía de antivirus descubrió en el análisis y la información que obtuvo es que las computadoras de la mayoría de los empleados de una organización están llenas de archivos con virus. Esto indica la prevalencia de dispositivos de almacenaje portables escasamente

[4] (Innovating in the Digital Economy) P 09, 15

resguardados y deterioro de parches en los sistemas de red. Las constantes infecciones de archivos expresa las dificultades que ha estado experimentando la empresas de América Latina para protegerse de los ataques y archivos maliciosos, lo que, nuevamente, muestra la poca conciencia de los empleados.

Perú, según the global information technology report se encuentra con 90% en el uso de la tecnología que indica que se mantiene en la misma posición que años anteriores por eso las pequeñas, medianas y empresas locales le dan poca importancia a la seguridad en los sistemas y redes de comunicación debido al poco interés que tienen las organizaciones y/o a la falta de recursos que tienen para invertir en equipos y personal especializado. Segun Richard Samans, Jefe del Centro para la Agenda Global y miembro de la Junta Directiva del Foro Económico Mundial de Ginebra indica en The Global Information Technology Report 2016 señala: *"Con la finalidad de fomentar la innovación y seguridad en las tecnologías de la información punto clave para prosperar en un mundo digitalizado y la emergente como la Cuarta Revolución Industrial el gobierno de Perú necesita con urgencia reforzar esfuerzos para mejorar sus entornos regulatorios y de innovación".*

El Grupo Suez es una compañía transnacional con inversiones y proyectos en Perú, las oficinas de Suez se encuentran ubicadas en Av. República de Panamá 3490, San Isidro 15047, cuenta con más de 600 colaboradores que trabajan para preservar los recursos en esta extensa zona geográfica. Cuenta con las áreas de Finanzas, Ingeniería, Comercial e Innovación Tecnológica que dan continuidad a los proyectos y procesos de la compañía.

El Grupo Suez no cuenta con un modelo de seguridad en su red de comunicaciones, que este alineado a una metodología de desarrollo de redes LAN, esto ha desencadenado que hoy en día la empresa pague las consecuencias, a continuación se describe la problemática:

- Los procesos de las áreas del grupo Suez no están alineados a controles de seguridad de ninguna norma técnica lo que coloca a la red en un punto vulnerable

- Se ha detectado que los usuarios acceden a páginas que no tienen que ver con las funciones laborales que se le fue asignado, el uso excesivo del internet, esta acción hace que el ancho de banda se vea limitado afectando a las aplicaciones que manejan las áreas de finanzas e ingeniería. Asimismo, no cuenta con un control de acceso a internet.

- El área de tecnologías no cuenta con ningún mecanismo o aplicativo que controle el acceso de usuarios a internet. Las interrupciones constante de los aplicativos CONCAR (sistema de contabilidad) y STARSOFT (sistema de planillas), se ha detectado que esta incidencia es debido a la saturación del canal del ancho de banda de la red LAN, lo que impide el normal funcionamiento del aplicativo, dejando indisponible en algunas ocasiones el flujo de la información por la red LAN.

- La falta de un modelo de seguridad con mecanismos de protección en su red LAN trae como consecuencia que no se puede tomar decisiones a nivel de la gerencia respecto a la asignación de tareas a los empleados. Es preocupante esta situación, por esta razón el Director General de la compañía tiene que colaborar con recursos técnicos y personal para la solución de este problema que puede traer grandes pérdidas financieras y, de tiempo siendo hoy en día un recurso muy valorado.

Ante esta realidad en este proyecto de investigación se pretende desarrollar un modelo de seguridad para prevenir la inseguridad de información alineado a los controles de seguridad de la ISO/IEC 27002:2013, ello con el fin de mitigar los problemas técnicos que actualmente tiene el Grupo Suez.

Figura 5: Ataque Cibernético a Ministerio Interior Perú

Fuente: Diario Gestión, Diciembre 2017

Figura 6: Rankig de Países Amenazados

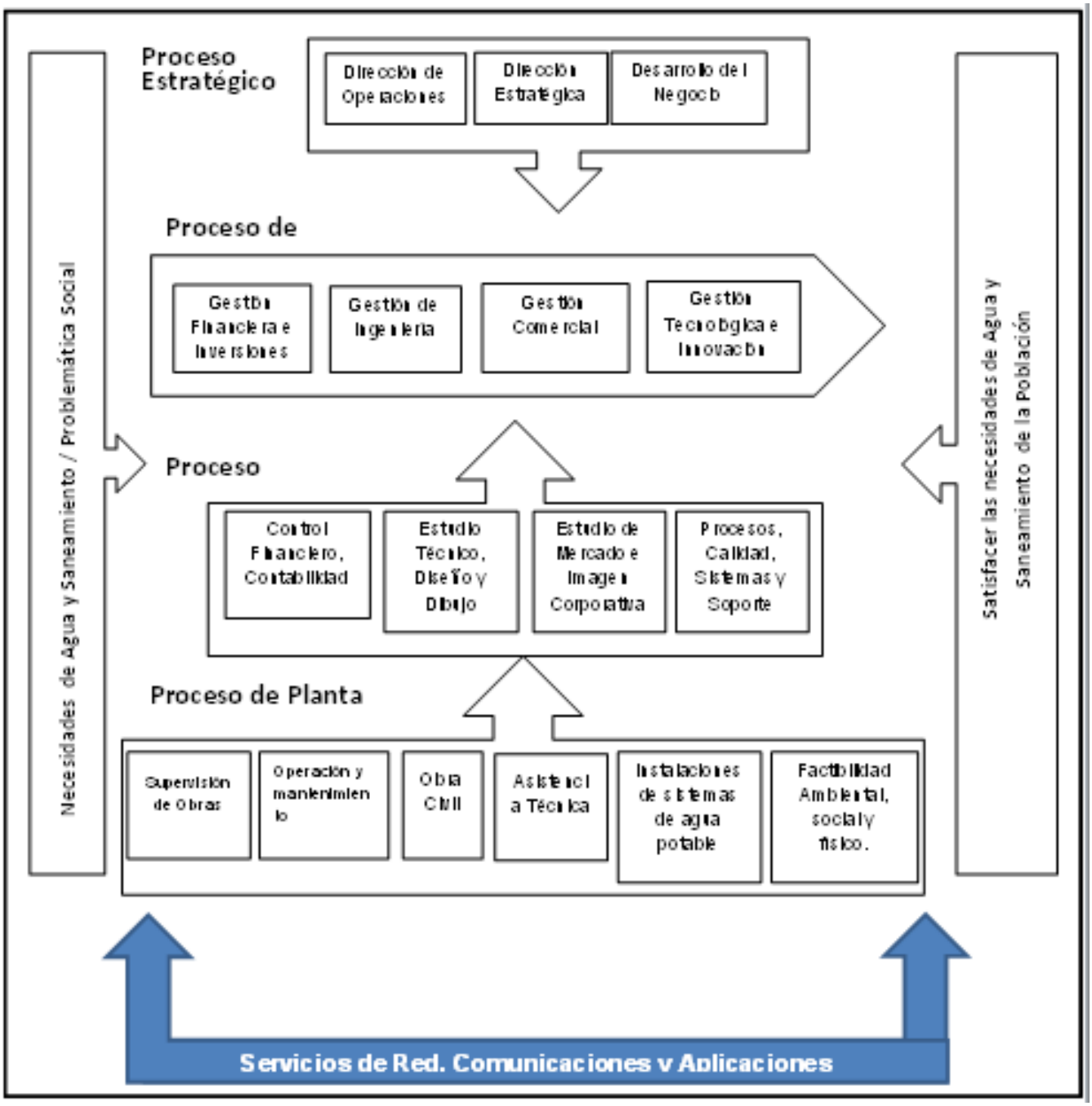
Fuente: Diario La República, Octubre 2015

Tabla 3: CAUSA - CONSECUENCIA DE LA PROBLEMÁTICA EN GRUPO SUEZ

CAUSA	PROBLEMÁ DE ESTUDIO	CONSECUENCIA
• Falta de personal especializado para desarrollar el sistema de seguridad. • Desconocimiento de parte del personal técnico. • No hay un diseño para estructurar la red de manera lógica. • Falta de comunicación de la problemática hacia la gerencia. • No se cuenta con recursos de TI.	**Lugar:** Grupo Industrial SUEZ **Quienes:** Las estaciones de trabajo (PCs). **Problemática:** No tienen un modelo de seguridad para controlar el tráfico de la red LAN.	• Que los servicios de TI del grupo SUEZ se interrumpan, lo que generaría un malestar del personal y acumulación de trabajos, ante esto los empleados tendría que quedarse más horas/días por lo que la empresa tendría que cubrir en alimentación y movilidad del personal generando costos para la empresa. • Se paralizaría las órdenes de trabajo para el personal (operario) en campo, ya que no podría tomar lecturas de los medidores de agua en los domicilios. • Se paralizaría la inspección técnica domiciliaria ante un reclamo por una facturación alta. • Se obtendría datos erróneos al momento de hacer las mediciones de consumo en un domicilio, dicha información podría ocasionar que se genera una facturación elevada. Ante esto se vería afectada una familia. • Perdida de información financiera, planes de proyecto, cartera de clientes, propuestas de ingeniería de futuros proyectos y propuestas económicas para ser presentado a los clientes que tiene el grupo industrial SUEZ.

Fuente: Elaboración propia

Tabla: Mapa de Procesos del Grupo SUEZ



Fuente: Elaboración propia

1.2 Trabajos Previos

1.2.1 Nacionales

Cabanillas Chávez, J. C. (2015). Propuesta de implementación de control de tráfico de la red con linux para optimizar la eficacia de servicios de TI en una Universidad privada de la Ciudad de Cajamarca Perú.

En ésta investigación se plantea el análisis y estudio de las varias Arquitecturas de Calidad de Servicio, como: Servicios Integrados (IntServ), que se basa en garantizar QoS a través de la reserva de recursos extremo a extremo para cada flujo, y la arquitectura Servicios Diferenciados (DiffServ), en donde se provee a ciertas estudios o protocolos, determinadas prioridades sobre la red. Se describirá las posibilidades que ofrece el sistema operativo LINUX, dentro del networking para optimizar los servicios de TI, revisando detalladamente teoría de colas y los mecanismos usados para control de tráfico, como son: scheduling, policing, Clasifying, etc. También describiremos de forma detallada el tema de colas, haciendo énfasis en aquellas que se pueden aplicar en el campo de control de tráfico de la red. Abordaremos el tema de enrutamiento avanzado con LINUX, y su aplicabilidad al control de tráfico, presentando las herramientas con que cuenta el sistema operativo con Kernel 2.6.x., que incluye IPTABLES el cual utiliza métodos de marcado de paquetes en un firewall, e IPROUTE2, donde veremos el uso de la utilidad (Traffic Control) que admite hacer el vigilancia de tráfico de la red, aplicando los conceptos como disciplina de colas, clases y filtros. Al término se planteara una propuesta que mejore el rendimiento de los servicios de TI, y que mejore la eficacia de los procesos de la Universidad.

Los resultados obtenidos posterior a la implementación, fueron satisfactorios, ya que en uno de los puntos aumento el consumo de la banda ancha del protocolo HTTP en un 46.1%.

Se perfeccionó la disponibilidad de los servicios de TI con resultados satisfactorios en base a los parámetros recomendados por la ITU-T en su apartado G.114 (Ancho de Banda, Latencia y Tasa de pérdidas), mejorando el consumo del ancho por parte de las aplicaciones y protocolos específicamente en la utilización del protocolo http en un 46.1%. En la medición de la latencia de la red se obtiene que está por debajo de los 150 ms teniendo un nivel aceptable para el trabajo correcto de la red de datos y la Tasa de Perdidas en la red LAN está por debajo del 1% lo que indica que existe una buena calidad de transmisión de datos en el enlace de la red.

Izquierdo Cabrera, J., & Tafur Callirgos, T. E. (2017). Mecanismos de seguridad para contrarrestar ataques informáticos en servidores web y base de datos. Universidad Señor de Sipán.

Izquierdo Cabrera en esta investigación realizó la comparación de mecanismos de seguridad que fueron capaces de contrarrestar ataques informáticos, con el propósito de capturar información de los intrusos y aumentar la seguridad en los servidores web y base de datos. Se identificó los sucesos de seguridad de la información, encontrando entre ellos a los ataques informáticos con mayor impacto en servidores. Estos fueron analizados y posteriormente se implementó sus mecanismos de seguridad en el diseño de la red establecida. Se implementaron los mecanismos de seguridad, establecidos por los investigadores, el primer mecanismo constó con la clonación de una red espejo virtual (Honeynet) autocontenida, así mismo se implementó el segundo mecanismo Snort en Kali Linux. Como resultados de la investigación se logró analizar y estudiar el impacto que ocasionaron los ataques, teniendo en cuenta el tiempo que queda indisponible el servidor, el mecanismo Honeynet obtuvo el menor tiempo de 0,8 segundo, frente a Snort que obtuvo 1,0 segundos. Así mismo se obtuvo como resultados el tiempo de respuesta que el mecanismo Snort logró reaccionar al 3,8 segundos, mientras que Honeynet reaccionó 3,6 segundos y rendimiento de los mecanismos de seguridad por cada ataque, se logró obtener un 97,5% de precisión, 99,2% de sensibilidad, 97% de especificidad y el 98,3% de exactitud en el mecanismo de seguridad Honeynet de generación III virtual autocontenida, frente al 97,9% de precisión, 98,0% de sensibilidad, 97,6% de especificidad y un 98% de exactitud del mecanismo Snort. A través de la investigación se hará mención de la problemática actual y las vulnerabilidades encontradas en los servidores especificados.

De la investigación y pruebas llevadas a cabo, ambos mecanismos detectaron y lograron contrarrestar los ataques DoS y exploración de vulnerabilidades en servidores web y base de datos. El mecanismo de seguridad Snort en Kali Linux, llegó a ser más preciso al momento de detectar el tráfico malicioso y el tráfico normal, refiriéndose a la especificidad. Mientras que el mecanismo de seguridad Honeynet obtuvo mayor porcentaje de exactitud y capacidad en la clasificación del trafico normal (sensibilidad). Por tanto, con el conocimiento y estudio, las herramientas que se utilizaron para la ejecución de las unidades de seguridad son relativamente factibles y rápidas de configurar, su administración se vuelve más sencilla a través de diferentes módulos que disponen de interfaz gráfica.

Paucar Falcón, b. h. (2017). Implementación de un Servidor de Seguridad Bajo el S.O GNU/Linux basado en la ISO 27002: 2013 Para mejorar la red de área local del área administrativa del hospital de contingencia Hermilio Valdizán Medrano de Huánuco, 2017. Universidad de Huánuco.

El actual tesis de investigación tuvo como propósito implementar un servidor de seguridad utilizando el sistema operativo GNU/Linux bajo los controles del ISO 27002:2013, en el Hospital de Contingencia Hermilio Valdizán Medrano de la ciudad de Huánuco en el año 2017. En cuanto a la metodología se planteó bajo el enfoque cuantitativo, y el tipo aplicativo; porque se utilizó la tecnología para la solución de un problema, así mismo se empleó el diseño pre experimental de pre y post test se llevó a cabo un experimento en condiciones controladas. La población estuvo conformada por 320 empleados del área administrativa del Hospital de Contingencia Hermilio Valdizán Medrano de la ciudad de Huánuco, y se determinó la muestra de forma no probabilística, de los cuales se permitió evaluar algunos controles técnicos en base a las actividades de los trabajadores en la red interna. En cuanto a la recolección de datos se usó la estadística descriptiva mediante el uso del software SPSS. Se utilizó el sistema operativo GNU/LINUX para dar soporte a la aplicación del servidor de seguridad usando los controles específicos números: 13.1.2 y 9.4 del ISO 27002:2013, se llevaron a cabo las pruebas de forma satisfactoria y cumpliendo el objetivo de dar seguridad a la red de área local del área administrativa del Hospital mediante la implementación de dicho servidor.

La Implementación del servidor de seguridad para mejorar los accesos a los recursos de la red interna y externa del área administrativa del Hospital de Contingencia Hermilio Valdizán Medrano de Huánuco, ha sido favorable y exitosa ya que se logró minimizar la cantidad de conexiones innecesarias, la cantidad de uso de MB, y la cantidad de acceso a sitios web no autorizado y por ende se logró una mayor productividad por parte de los trabajadores ya que anteriormente a la aplicación los trabajadores usaban el tiempo de sus labores para acceder a páginas no autorizadas, descargar contenido no autorizado generando cuellos de botella en la red, también modificando y eliminando información del servidor sin autorización.

Por tanto, Paucar Falcón concluye que el uso de un servidor de seguridad que administra los recursos de la red, es preciso dentro de cualquier empresa por cuestiones de seguridad, facilidad de gobierno de archivos, gestión de cuentas de usuario y reglas de entrada de los mismos, concentración de la información, habilidad para compartir archivos.

1.2.2 Internacionales

Guevara Aulestia, David Omar, Sánchez Cunalata, David Fernando (2017) Implementación de un sistema de monitoreo y protección de datos en la red de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

El propósito del actual labor de tesis es Implementar un Sistemas de Monitoreo y protección de datos en la red de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, con la finalidad de analizar y dar solución a los inconvenientes planteados en la investigación, para optimar el ancho de banda y cumplir a cabalidad la productividad operativa de la FISEI en beneficio de la comunidad Universitaria. En la actualidad por los ataques al ancho de banda, la falla de los dispositivos y el descontrol de usuarios conectados a la red ha dado lugar a que se promueva la implementación de un Sistema de Monitoreo y protección de datos en la red de la Facultad de Ingeniería en Sistemas Electrónica e Industrial mejorando el control interno y externo, se recopiló información de los dispositivos de red y equipos de cómputo de los laboratorios y áreas administrativas, además se configuró los sistemas MUNIN, MRTG y CACTI para su monitoreo, los mismo que emiten alertas inmediatas de fallas en los distintos dispositivos de la red, así mismo, una vez realizado lo detallado, se procedió a realizar un cuadro comparativo para el análisis de los sistemas de monitoreo ya para finalizar el actual plan de investigación se implementó un modelo de seguridad Suricata mitigando la problemática de ancho de banda como las actividades no autorizadas que provoquen la degradación en la red.

En esta investigación los autores han desarrollado un sistema de monitoreo de la red de datos eficaz en cuanto a la detección de fallos y congestionamiento, debido a la utilización de sistemas de monitoreo implementados en la red de la FISEI en el sector de administración de redes. Se efectuó el análisis de las herramientas de monitoreo más idóneas para la observación de la red de datos de la FISEI, por lo cual el sistema Munin fue el más idóneo cumpliendo con todas las proyecciones necesarias para la detección de fallos y congestionamiento en el ancho de banda. En relación a lo estudiado a lo largo de la presente proyecto de investigación se determinó establecer mecanismos de control y protección de datos para optimar el rendimiento de la red de la Facultad de Ingeniería en Sistemas Electrónica e Industrial de la Universidad Técnica de Ambato. Respecto al desarrollo del Sistema de Prevención de Intrusos e Identificación de intrusos se implementó Suricata, herramienta necesaria para protección de cualquier arquitectura computacional ya que posee

características únicas que no se encuentran en otros sistemas de acuerdo a la comparación realizada en la Tabla 67 en la que se demuestra su superioridad en cuanto a sus peculiaridades técnicas.

Moscote Medina, Rafael Luis (2017) Sistema de detección y prevención de intrusos ips para la vlan de servidores de la Sociedad Minera de Santander S.A.S. en Bucaramanga (Colombia). 108 P.

La presente tesis de Grado fue elaborado para optar al Título de Especialista en Seguridad Informática, consiste en la instalación de un Sistema de detección y prevención de intrusos basado en red para la Sociedad Minera de Santander S.A.S en Bucaramanga (Santander), este sistema permite el análisis del tráfico en tiempo real que ingresa a la Vlan de servidores en búsqueda de posible ataques y anomalías en las cabeceras de paquetes y protocolos de la capa de red (IP, UDP, TCP e ICMP) utiliza un lenguaje de reglas para detección y bloqueo de intrusiones, realizando un análisis de protocolos con información de la IP de donde se originó el ataque y hacia qué destino y puerto. Para la elaboración de este proyecto fue necesario aplicar la metodología investigativa y conocer los sistemas de detección y prevención de intrusos, luego se recopiló la información del esquema de red actual de la empresa y se propuso una nueva topología que incluya un IPS detrás del Firewall, teniendo en cuenta que las amenazas provienen de la propia red interna de la empresa, se llevaron a cabo pruebas y se comprobó su correcto funcionamiento.

Con este proyecto se fortaleció el mecanismo de seguridad en la red de datos de la empresa Minesa, se comprobó que no cuenta con un sistema de detección de intrusiones a nivel interno de su red de servidores que permita descubrir y bloquear acciones y alertar de comportamientos anómalos a nivel interno. También, ayudó a prevenir el escaneo no autorizado a puertos de los servidores y facilitó la remediación de problemas de seguridad interno y en la definición de reglas que garanticen la reserva, disponibilidad e de la información.

Bravo Mora Briggitte Stephanie, Daudo Nieto Adriana Anabel (2017) Diseño de Gestión de Seguridad de la Información en Base a la Norma ISO 27002 y al estudio de situación actual de la empresa proveedora de internet "POSORJA en acción CIA. LTDA."

Ambos estudiantes desarrollaron este proyecto en la empresa "Posorja en acción S.A." que se dedicada a proveer servicios de internet a la población, así como también a dar soporte tecnológico a sus clientes. Sus servicios vinculan muchas actividades que implican que la seguridad de la información sea demasiado importante. Poseen los equipos necesarios, pero estos no tienen las debidas protecciones es decir que están expuestos a amenazas. La finalidad de este trabajo es proveer el diseño de la gestión de seguridad que sirva como guía para los gestores del centro de cómputo de la empresa y así poder mitigar los riesgos existentes, también para crear controles que permitan

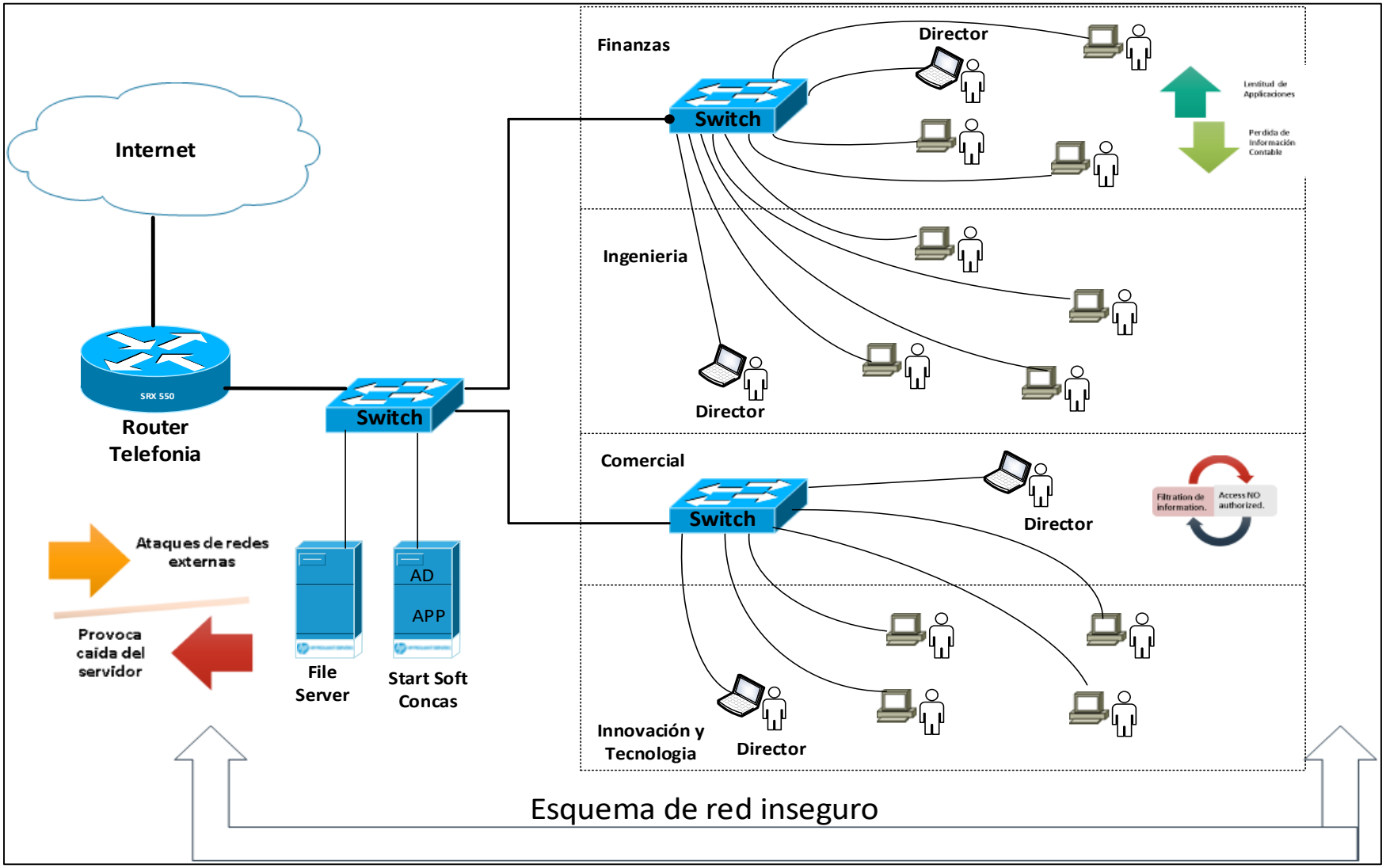
evitarlos. Se realizó el diseño en basado al estudio de la contexto actual y a la selección de los controles pertinentes de la norma ISO 27002, se usará como metodología MAGERIT que utiliza a modo herramienta el software PILAR para el análisis y gestión de riesgo permitiendo identificar amenazas. Este diseño ayudara que los miembros de la empresa tomen conciencia del peligro que se encuentran, y que deben tomar medidas preventivas que servirán para proteger los activos de la empresa con el fin de ser menos vulnerable ante posibles ataques y servirá como referencia para empresas que se dediquen a una actividad similar.

En esta investigación se utilizó MAGERIT como metodología para el estudio del contexto actual de la empresa y siguiendo los pasos que contiene para obtener los resultados del estudio, esto permitió llevar un orden durante el proceso del análisis. También se realizó la evaluación de la escenario actual de la compañía en cuanto a la seguridad de la información para esto se utilizó la herramienta PILAR como ayuda para el estudio de escenario presente, y se realizaron ataques para vulnerar los tres columnas de la seguridad de la información como la integridad, disponibilidad y confidencialidad, como resultado se pudo evidenciar la falta de controles ya que los ataques fueron exitosos es decir que para cualquier intruso sería un reto fácil obtener información de la entidad. En resumen, se analizó la norma ISO 27002 para seleccionar los dominios pertinentes y según el estudio de situación actual se listó las amenazas para cada activo identificado dentro de la empresa, esto sirvió para diseñar los controles con sus respectivas recomendaciones que puedan ser puestos en práctica. Este diseño de controles podrá servir como referencia para otras empresas ISP que deseen mejorar sus operaciones internas y también para que tengan como referencia un documento que señalará las vulnerabilidades básicas que una entidad dedicada al mismo campo pueda tener. Finalmente, el diseño de la misión de la seguridad de la información ayudará a la empresa a prevenir las amenazas futuras de acuerdo con las recomendaciones elaboradas según la selección de los controles de la norma ISO 27002 en base a las amenazas identificadas en el estudio de escenario actual de la empresa para garantizar la seguridad de la información.

Ruiz Osorio, Daniel Fernando (2015) Implementación de un esquema de seguridad basado en herramientas Linux para la Cooperativa de Ahorro y Crédito Microempresas de Colombia

El trabajo proyecta una alternativa para la ejecución de un proyecto de seguridad basado en equipos LINUX, que admite afirmar los puntos críticos de una infraestructura de cara a Compañías PYME. La mezcla de herramientas LINUX y Windows, dispuestas bajo estándares y protocolos fundados, permiten que se enlacen los aspectos notables de cada una de las plataformas, y que su interacción consienta un esquema de seguridad óptimo con mínimos costos de infraestructura.

Figura 7: Problemática actual en el Grupo SUEZ (esquema de red inseguro)



Fuente: Elaboración propio

1.3 TEORÍAS RELACIONADAS

1.3.1 BASE LEGAL (Normas Legales establecido en Perú)

Para la implementación de este proyecto se tendrán en cuentan las leyes en el Perú que protegen los datos y la integridad de los gobiernos informáticos y de las sanciones a las personas que hagan uso de manera fraudulenta de los sistemas informáticos y las redes de las empresas, pymes y grandes compañías.

El proyecto se fundamenta en la Ley N° 29733, la ejecución del proyecto estará acorde con las normas y requisitos legales de la actualidad. Por lo tanto, los registros que generará el sistema podrán ser requeridos como pruebas que ayudarán a localizar y sancionar a los responsables. Los siguientes son los artículos de Ley 30096 abarca el siguiente proyecto:

1.3.1.1 Protección de Datos Personales Ley de N° 29733

El esencia de la ley es garantiza el derecho fundamental a la defensa de datos propios, previstos en el artículo 2 numeral 6 de la constitución Política del Perú, atravesó de su apropiado método, en el marco de acatamiento de los demás derechos primordiales que en ella se examinan.

1.3.2 MARCO CONCEPTUAL

1.3.3 SOLICITUDES WEB

Es una petición de acceso a internet que una estación de trabajo (PC) realiza. La petición puede ser de cualquier página o contenido de búsqueda en internet. La aplicación se procesa por el lado del servidor, ejecutando conexiones bidireccionales o unidireccionales y síncronas o asíncronas con internet y formando o una respuesta en cualquier lenguaje, el contenido recibido se muestra a través de un navegador web, para la transmisión de los datos suele manipular algún protocolo. (Belloch Ortí, 2015, Pag. 105)

1.3.4 SISTEMA DE PROTECCIÓN DE REDES LAN

1.3.4.1 Servidor Proxy.

(GOMEZ, Álvaro, 2007, Pags. 401-402). Estos fueron concebidos de forma autónoma por Jed Haile y Vern Paxon para resolver ambigüedades en la monitorización pasiva de redes de ordenadores. Un sistema de prevención de intrusos, al igual que un Sistema de Detección de Intrusos, anda por medio de módulos.

1.3.4.2 Características

Capacidad de reacción automática ante acontecimientos.

Aplicación de nuevos filtros conforme detecta ataques en avance.

Pequeña atención.

1.3.4.3 Ventajas

No se puede ser buenamente eludido o la ventaja primordial de esta habilidad radica en la actualización y también en la gran cantidad de firmas que se encuentran en la base N-IDS. Pero, cantidad no siempre significa calidad. Por ejemplo, los 8 bytes "CE63D1D2 16E713CF", cuando se colocan al inicio de una traspaso de datos UDP, indican un tráfico Back Orifice con una clave predeterminada.

1.3.4.4 Desventajas

- En los proxys no utilizar usuarios y contraseñas que son de bancos o correos personales.
- El guardar páginas de los usuarios que ya visitaron puede suponer un trasgresión a la intimidad de algunas personas.
- Ingresar a internet por medio de un servidor proxy, en vez de ingresar directamente sin filtros a internet, restringe el hecho de realizar operaciones avanzadas en aplicativos web que utilizan puertos lógicos específicos.

1.3.4.5 Tipos de Ataques Informáticos

(Gómez, 2011, p. 204). En su libro da a conocer algunos tipos de ataques informáticos existentes, los cuales se pueden diferenciar por ataques activos, que son los que producen grandes cambios en la información y también los ataques, lo cuales se encargan de limitar el uso de los recursos para acceder a la información guardada o intercambiada por el sistema.

(Ramos A. B. y Ribagorda G. A., 2004, p.46) También presentan una relación de los primordiales tipos de ataques informáticos contra redes de datos.

a) **Ataques externos:** Son instruidos por un individuo o grupos trabajando desde afuera de una empresa. Ellos no tienen acceso acreditado al sistema o red de computadoras de dicha empresa. Reúnen información para así abrir camino dentro de la red, principalmente lo hacen a través de internet o servidores por marcado.

b) **Ataques internos**: Estos tipos de ataques son los más comunes y catalogados como peligrosos, los ataques principalmente son iniciados por usuarios con acceso acreditado a una red de datos, comúnmente por usuarios internos a la empresa, o usuarios despedidos descontentos.

c) **Ataques a nivel de sistema**: Este tipo de ataque llega a atacar directamente al sistema operativo del servidor especificado, intentando obtener privilegios de administrador o más conocido como root mediante un terminal remoto. Estos ataques se basan en vulnerabilidades a la hora de configurar las políticas de acceso al servidor a través de un servicio mal configurado (como por ejemplo servicios Telnet y SSH), o bien explotar servicios vulnerables permitiendo desbordamiento de buffers que puede permitir ejecutar comando en el sistema operativo.

d) **Ataques de fuerza bruta:** Este tipo de ataque se realiza para "adivinar" una clave secreta tratando con todas las mezclas viables de caracteres hasta encontrar la correcta. Y es que acceder a las contraseñas de los usuarios no es fácil, ya que se guardan de manera encriptada y la única alternativa es adivinarlas u obtener mediante el uso de "sniffers" – programas que interceptan las comunicaciones y registran las contraseñas, sin embargo, cuando estas técnicas fallan, los hackers recurren a la fuerza bruta.

e) **Ataques DoS.** Consiste en diferentes acciones que permite colapsar determinados equipos o redes informáticas para frenar que puedan ofrecer sus servicios a sus clientes. Uno de los protocolos que podría verme más afectado por esta debilidad en TCP es BGP utilizado para el intercambio de información de enrutamiento entre las redes de los proveedores de acceso a Internet provocando la 45 desconexión de todas las redes que dependan de un router vulnerable al ataque. Para evitar estos problemas, se puede utilizar algún sistema que permita autenticar los dos extremos de la comunicación.

f) **Denegación de Servicio:** (Castro, M., Díaz, G. y Alzórriz, I. 2014) Denegación de servicio, buscan dejar no disponible un servicio, una red o un sistema, agotando los recursos como el ancho de banda, espacio en disco, conexiones, etc. Este tipo de ataque no necesita ningún acceso previo al sistema, también los Distributed denial of service (DDoS) vienen a ser ataques prácticamente imparables.

1.3.4.6 Redes de área Local

(Tanenbaum, 2003) Las redes de área local son redes de pertenencia privada que se hallan en un solo edificio de pocos kilómetros de extensión. Se utilizan largamente para enlazar computadoras personales en oficinas de una empresa para compartir recursos (por ejemplo, impresoras) e tratar información. Las LANs son disparejos de otros tipos de redes en tres aspectos: tamaño; tecnología de transmisión, y topología.

1.3.4.7 Ancho de Banda

(UNIÓN INTERNACIONAL DE TELECOMUNICACIONES, 2001). Una compostura del tamaño de transmisión de datos, enunciada generalmente en Kilobits por segundo (kbps). Indica la capacidad máxima teórica de un enlace, pero este volumen teórico se ve reducida por elementos negativos tales como el retardo de transmisión, que pueden producir una avería en la calidad. Es determinante para examinar el comportamiento de la calidad en Redes de Área Local, en estas redes se debe de tener en recuento el beneficio de los dispositivos de interconexión según las capas del modelo OSI y su relación con la QoS.

1.3.4.8 Trafico de Red.

(UNIÓN INTERNACIONAL DE TELECOMUNICACIONES, 2001). Una medida de la capacidad de transmisión de datos, formulada totalmente en kbps o Mbps. Indica la volumen máxima teórica de una conexión, sin embargo esta capacidad teórica se ve reducida por elementos malos tales como el lentitud de transmisión, que pueden producir un avería en la calidad .

1.3.4.9 Neutralizar

(Giménez, María y Gómez, Julio, 2008, Pag. 20). “Neutralizar en un sistemas de prevención de intrusos es una respuesta que se activa ante los ataques. El término de respuesta activa se aplica a cualquier función que altera o bloquea el tráfico de red como resultado de los programas de detección de abuso. El propósito de la repuesta activa es automatizar la respuesta a un ataque detectado y minimizar o idealmente bloquear los efectos malignos de los intentos de intrusión impidiendo la capacidad de acción del enemigo”.

1.3.4.10 Controles

Es un conjunto de rutinas a ejecutarse que nos admite dar un seguimiento a los activos más afectados dentro de una organización. Estos controles están sujetos a una política para disminuir los riesgos identificados, (Roa, 2013).

1.3.4.11 Auditoria

Alonso Rivas (1989) Es un análisis que se realiza con objetivo, crítico, sistemático y selectivo con el fin de evaluar la eficacia y vigencia del uso adecuado de los recursos informáticos, de la gestión computación y si estas han ofrecido el soporte adecuado
a los propósitos y metas del negocio. La Auditoría Informática corresponderá vislumbrar no sólo la valoración de los equipos de cómputo, de un sistema específico, sino que además habrá de evaluar los sistemas de información en general desde su ingreso, procedimientos, controles, archivos, seguridad y obtención de información.

1.3.4.12 Trafico de red

ANDREW L. RUSSELL (2013) Los paquetes recorren una ruta para ingresar a un sistema y para salir de él. En un nivel granular, los paquetes se reciben y se transmiten mediante los anillos de recepción (Rx) y de transmisión (Tx) de una NIC. Desde estos anillos, los paquetes recibidos se transfieren a la pila de red para su posterior procesamiento mientras los paquetes salientes se envían a la red.

1.3.4.13 Eficiencia

(Contreras, 2010). Es la capacidad de disponer de alguien o de algo para conseguir un efecto fijo.

La eficacia de los servicios que facilitan las tecnologías de la información y la comunicación (TIC) pasa por saber interesar mejor los recursos, inspeccionar y tramitar de forma ordenada y colaborar, haciendo así que sean también más competitivos.

1.3.5 SEGURIDAD DE LA INFORMACIÓN BASADO ISO 27002

1.3.5.1 IMPORTANCIA DE LA SEGURIDAD

(Javier Areitio, 2008. Pag. 5). La disposición, cada vez más imperioso, hacia la interconectividad y la interoperabilidad de las redes, de las máquinas de computadoras, de las estudios, e incluso, de las organizaciones, ha situado a la seguridad como un componente central en todo el progreso de la humanidad.

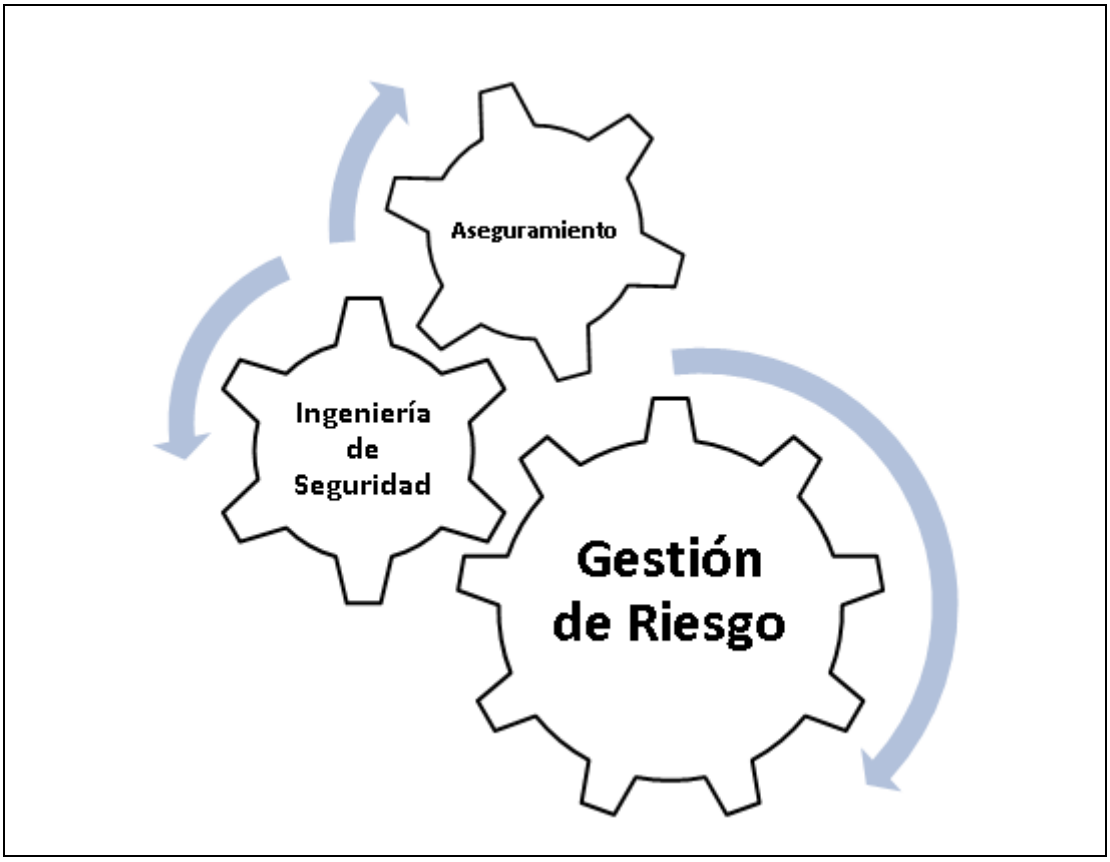
La seguridad ha pasado de utilizarse para preservar los datos clasificados de régimen en cuestiones militares o diplomáticas, a tener unas dimensiones incomprensibles y progresivas que incluye transacciones bancarias, acuerdos pactados, información personal, archivos médicos, comercialización y negocios por internet, domótica, inteligencia

ambiental y computación ubicua. Por ello, se ha imprescindible que las necesidades de seguridad permitidos sean tenidas en cuenta y se determinen para todo tipo de aplicaciones.

a) Áreas de Procesos de Seguridad

(Javier Areitio, 2008. Pag. 10). Todo modelo de madures divide la seguridad en 3 grandes áreas: transcurso de misión de riesgos, transcurso de ingeniería de seguridad y proceso de aseguramiento (Javier Areitio, 2008. Pag. 7). Estas no son independientes entre sí, pero es posible considerarlos por separado.

Figura 8: Procesos de Seguridad



Fuente: Seguridad de la Información autor: Javier Areitio

b) Servicios de Seguridad

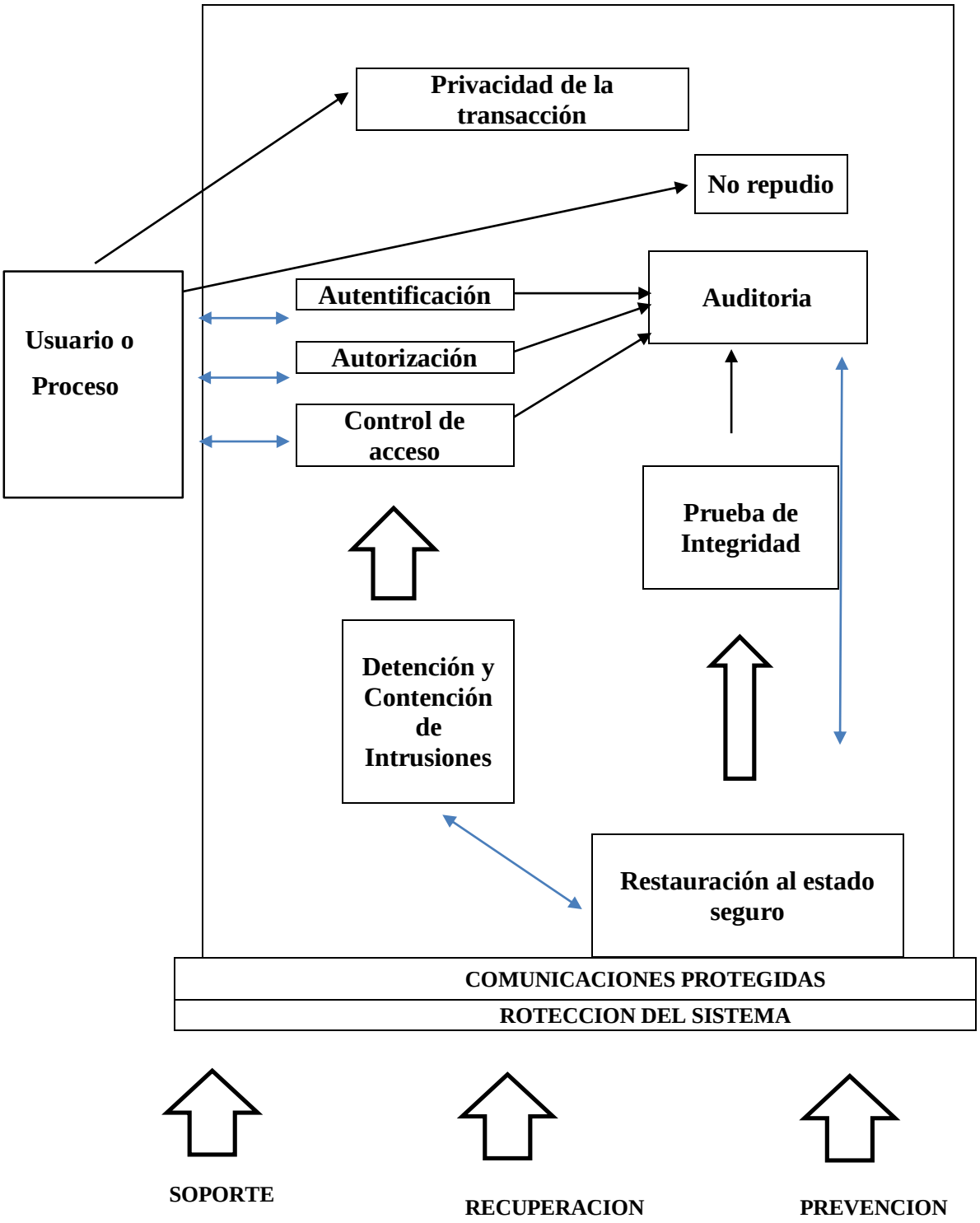
(Javier Areitio, 2008. Pag. 20). Los productos de seguridad admiten implementar la política de seguridad de una compañía. Se forman en los sistemas de información formada por redes, computadores y personas. Con el objeto de dar amparo a todas las entidades identificables (Javier Areitio, 2008. Pag. 11). Se describen los servicios:

- Servicios de disponibilidad-accesibilidad, servicios de identificación autentificación.
- Servicios de integridad, Servicios de soporte.
- Servicios de autorización control de acceso

c) Sistema de Seguridad

(Javier Areitio, 2008. Pag. 85) Un sistema de seguridad está basado en resguardar archivos, software, base de datos, redes y toda información relevante. Está creada para elaborar instrucciones y métodos que lleven a un insuperable nivel de seguridad, capaz de solucionar toda posible amenaza. Actualmente una red LAN cuenta con muchos peligros de seguridad que se deben evaluar y mitigar.

Tabla 7: Esquema de Seguridad



Fuente: Libro seguridad de la información autor: Javier Areitio

d) Elementos de Gestión de la Seguridad

(Javier Areitio, 2008. Pag. 58). En el transcurso de la administración de seguridad existen una serie de elementos involucrados siendo:

- **Identificación de todos los activos.**

  Son aquellos componente concernidos con el ámbito; como persona, edificios, instalaciones, equipos o suministro dependidos con los sistemas de TI como dispositivos de hardware y software, aparatos de comunicaciones de datos, pertenecidos con la información, ligados con funcionalidades de la organización, como la capacidad de facilitar un servicio, crear un producto, los activos intangibles, como la imagen de la organización, credibilidad y conocimiento adquirido.

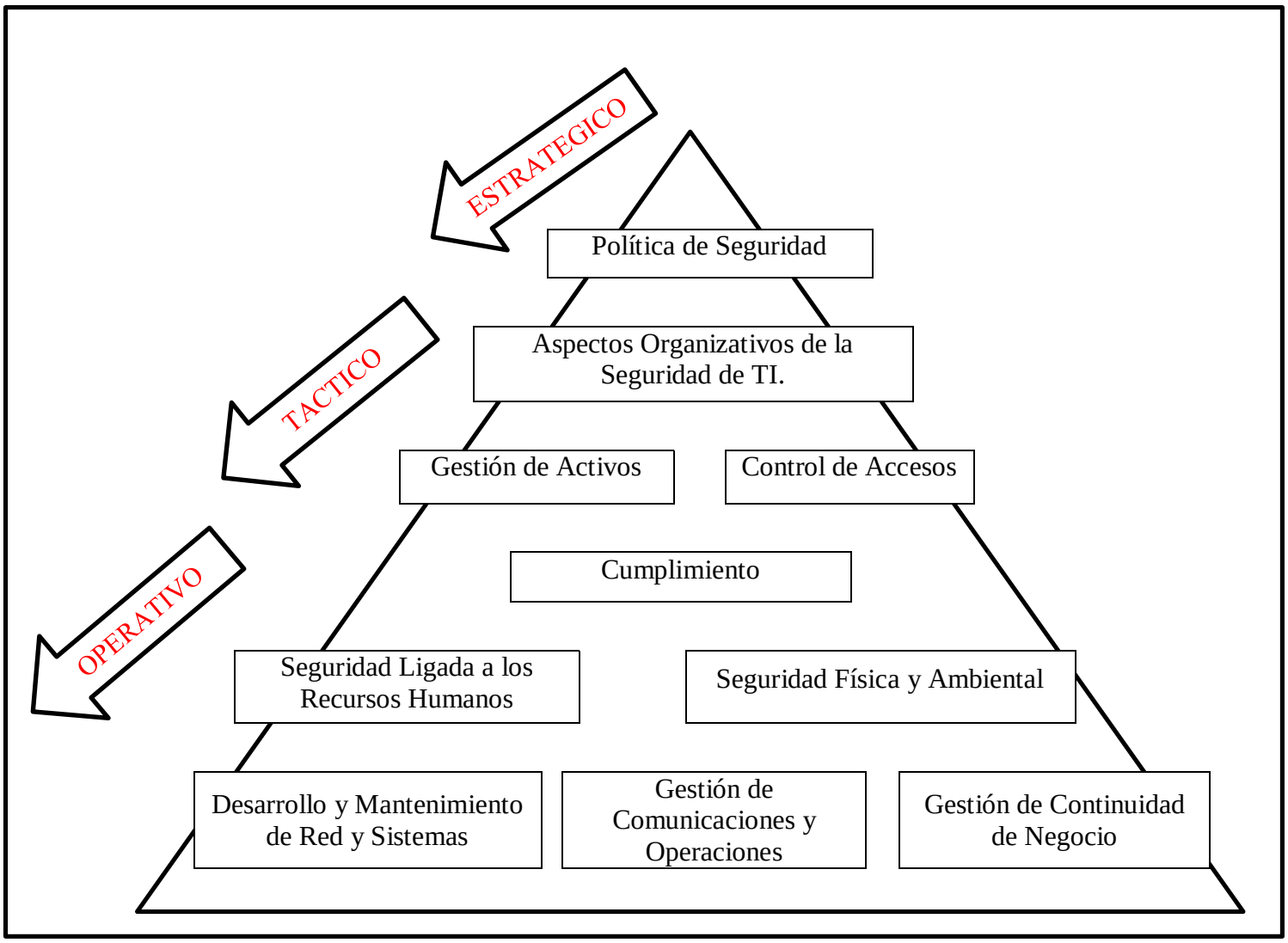
- **Identificación de amenazas de los activos.**

  Una amenaza puede causar un problema no deseado, que puede provocar daños o perdidas de todo tipo en la compañía, estos desgastes pueden proceder de una agresión directa o indirecta sobre una red o sistema de información. Las agresiones son en forma de revelación, destrucción, modificación no autorizada, de indisponibilidad o perdida de información.

- **Identificación de riesgos.**

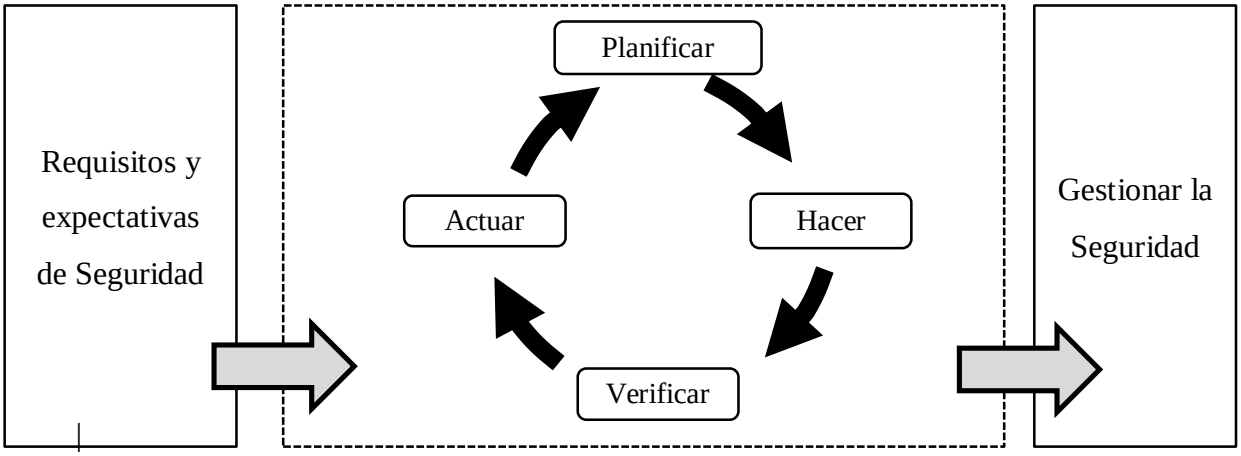
  El riesgo es la posibilidad de que se inicie un impacto explícito en un activo, en la organización. Este impacto se puede producir debido a que una amenaza explote vulnerabilidades para cuasar pérdidas o daños. Un entorno de peligro es aquel en el que una amenaza puede explotar una vulnerabilidad determinada exponiendo los activos a daños o pérdidas. El riesgo se caracteriza por una combinación de 2 factores: La posibilidad de que ocurra el suceso no deseado y su impacto. Cualquier modificación en activos, amenazas, vulnerabilidad puede tener efectos significativos en el riesgo. La rápida detección o el conocimiento de cambios en el sistema de red facilitan la toma de decisiones adecuadas.

Figura 9: Componentes de la Seguridad de la Información



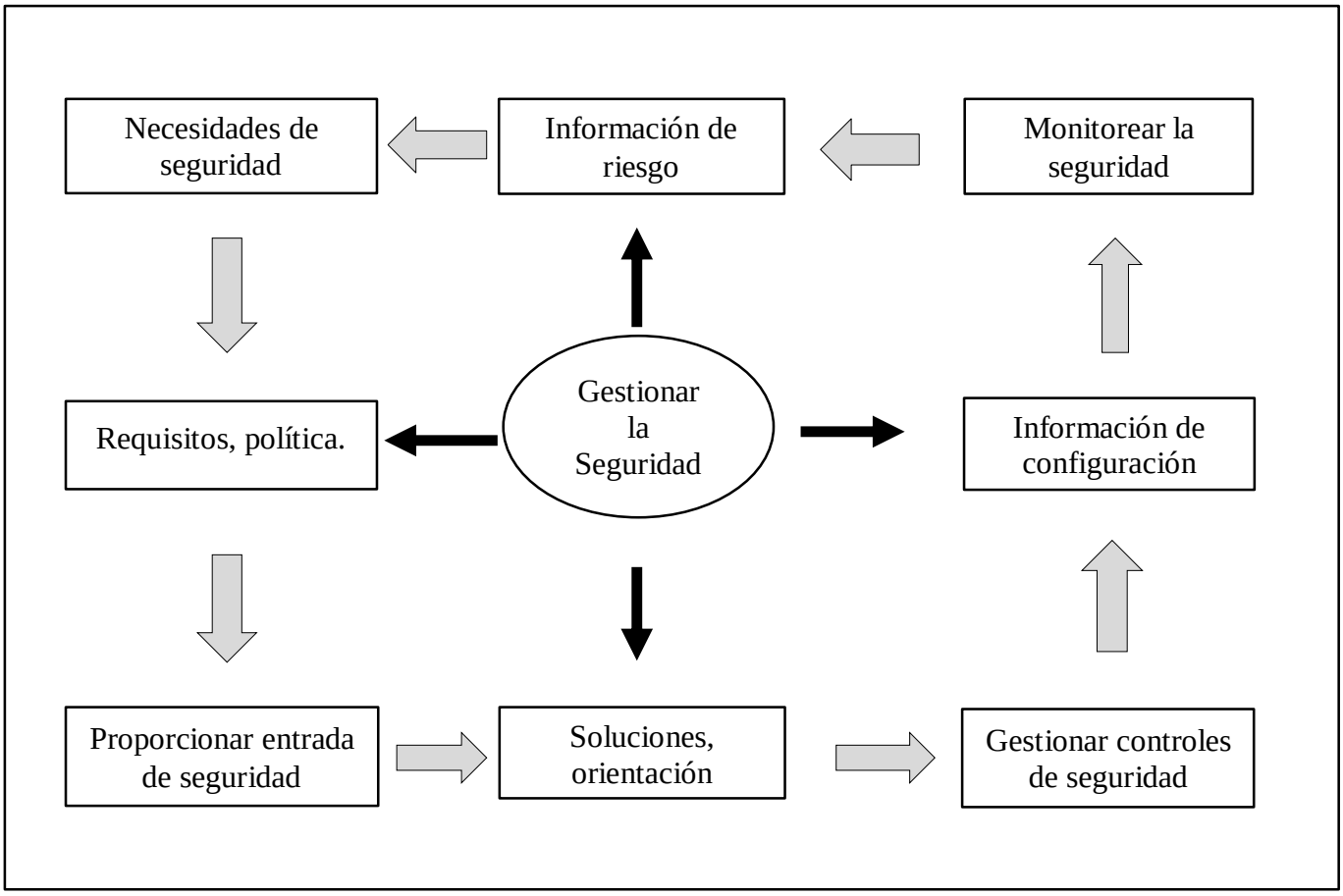
Fuente: Redes, informática y sistemas de información autor: Javier Areitio

Figura 10: Modelo PHVA aplicado a seguridad de la información



Autor: Edwards Deming

Figura 11: Objetivo de la Política en el Grupo SUEZ.



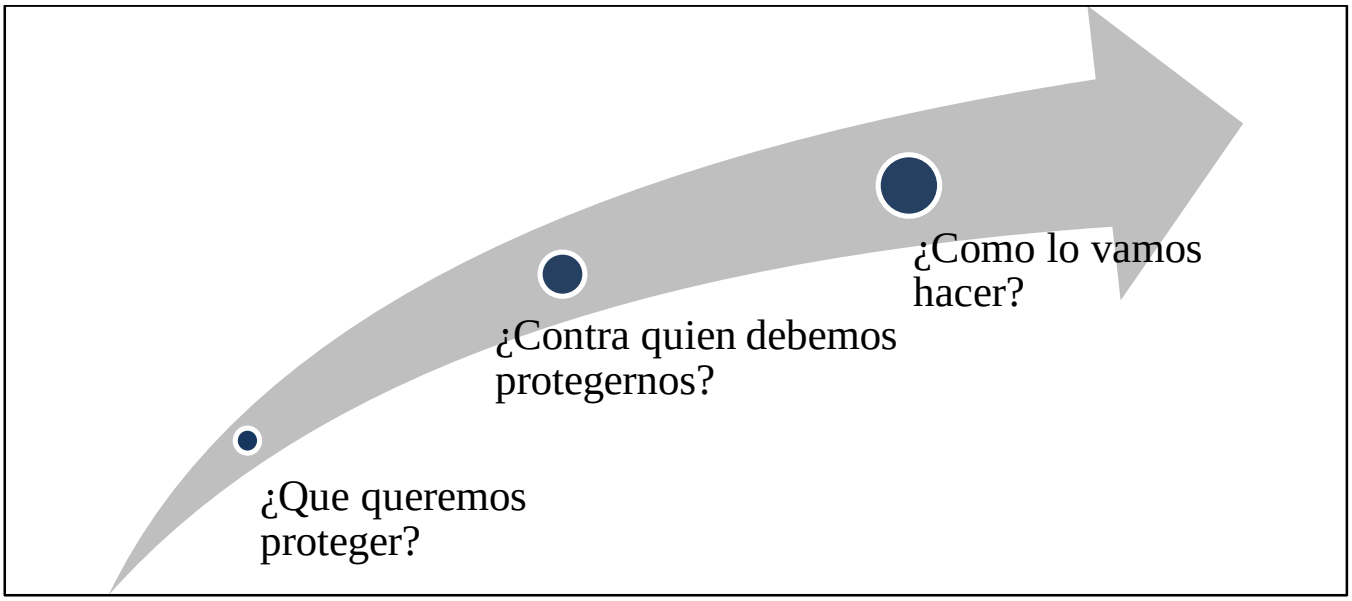
Fuente: Redes, informática y sistemas de información autor: Javier Areitio

1.3.5.2 ANÁLISIS Y GESTIÓN DE RIESGOS DE LA SEGURIDAD

En un entorno de interconexión o seguridad de la información, coexisten recursos humanos, expertos de infraestructura, organizativos o de gestión, que se encuentran exhibidos a peligros, que afectan a toda o una parte de la organización, como la inestabilidad política de un país o la ubicación de la empresa en una región sensible a terremotos, tornados o inundaciones.

Para reducir los efectos de un problema de seguridad, se realiza el llamado análisis de riesgos, palabra que hace referencia al transcurso necesario para responder a tres debatas básicas de la seguridad de una organización, "que es saber que queremos proteger, contra quien o que se quiere proteger y como lo vamos hacer". El análisis de riesgos constituye una parte clave de la gestión, es un proceso sólido en identificar los peligros que afectan la seguridad, establecer su magnitud e igualar las áreas que requieren salvaguardar.

Tabla 11: Preguntas para analisar un riesgo



Fuente: Sistemas de información autor: Javier Areitio

a) Análisis de riesgos

En la experiencia, existen 2 apuntes básicos a la hora de realizar un justo análisis de riesgos, uno cuantitativo y otro cualitativo.

El camino **cualitativo** de análisis de riesgo es de rutina muy usual en la actualidad, fundamentalmente entre las nuevas organizaciones consultoras de seguridad, en aquellas más especializadas en seguridad lógica, firewall, test de intrusión. Es mucho más simple que el

intuitivo que el cualitativo, ya que ahora no entran en juego posibilidades exactas sino simplemente una estimación de pérdidas potenciales. La seguridad en cualquier sistema debe estar siempre en consonancia con sus riesgos, sin embargo el proceso para determinar los controles de seguridad más apropiada y rentable es, a menudo, bastante complejo y, a veces, se convierte en una cuestión subjetiva.

El enfoque **cuantitativo** es, con discrepancia, el menos utilizado, ya que, en muchos casos, genera deducciones complejos o datos difíciles de calcular. Se basa en dos parámetros, que son la probabilidad de que produzca un suceso y una estimación del coste o de las perdidas.

El enfoque cualitativo

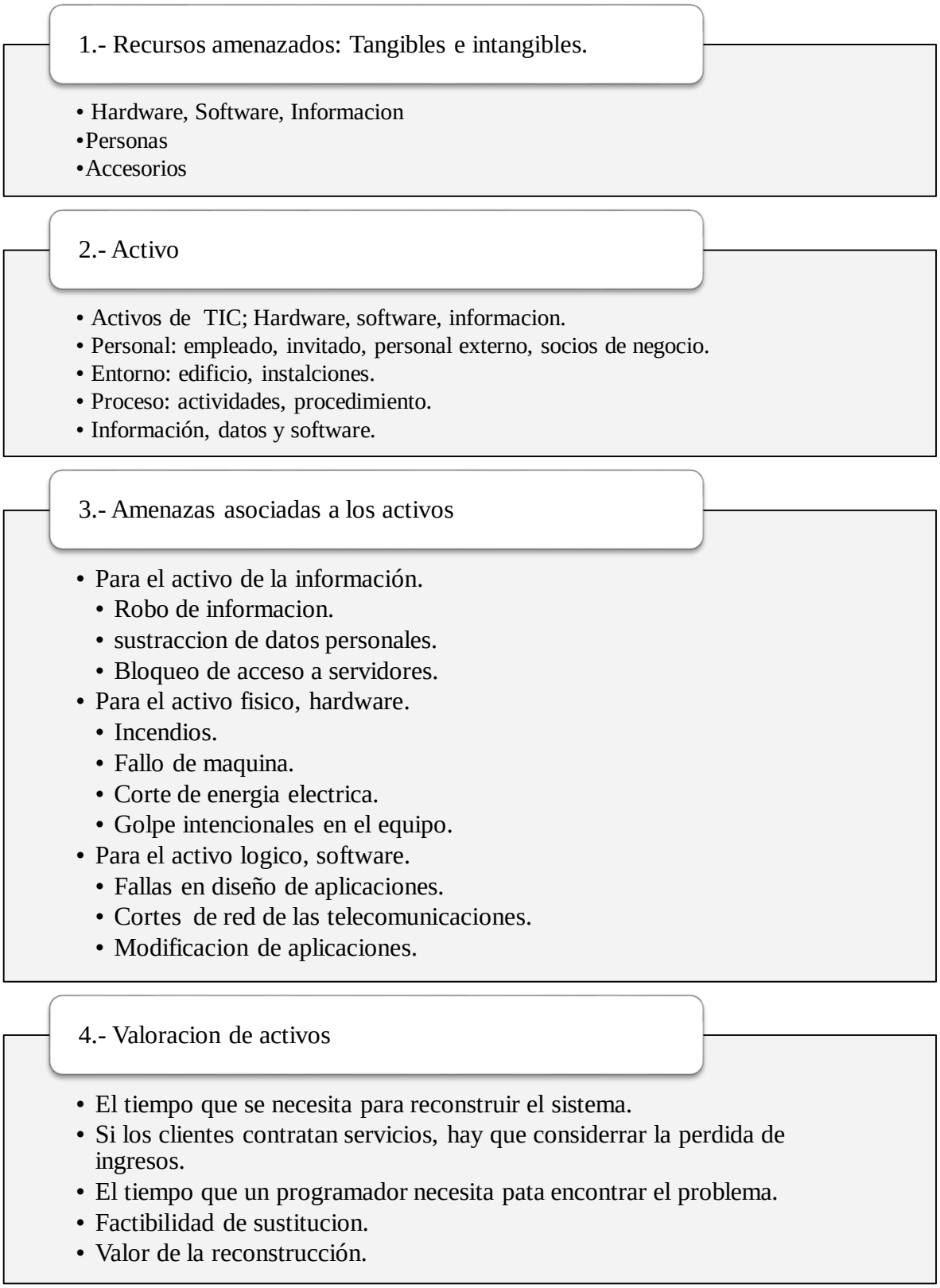
La técnica o dirección cualitativa es más adecuado para instalaciones pequeñas y el más utilizado en la actualidad.

- Riesgos de amenazas.
- Gravedad del ataque.
- Daño.

b) Identificación de Recursos

Como ya se ha dicho anteriormente, los activos de una empresa u organización son, cada día más numerosos. Algunos son visibles y otros no. Es indudable que algunos son de más valor que otros y, por tanto, es necesario establecer una lista de prioridades, si una organización desea subsistir, debe proteger sus activos frente a cualquier tipo de contingencia tanto externa como interna.

Figura 12: Identificación de Recursos Frente a una Falla de Seguridad

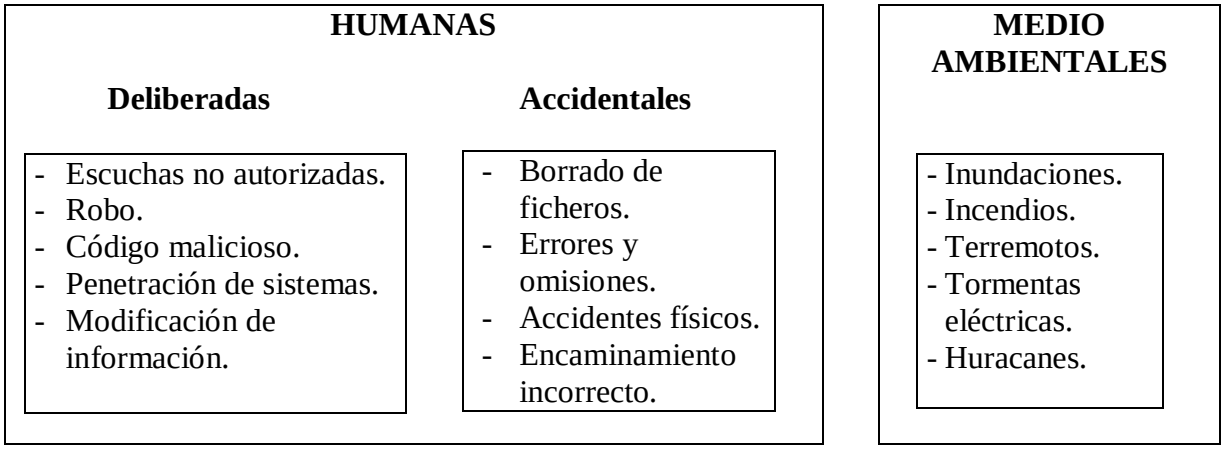


Fuente: Redes, informática y sistemas de información autor: Javier Areitio

c) Explotación de Amenazas

La explotación de amenazas consiste en aprovechar las deficiencias o debilidades de un sistema para lanzar un ataque.

Figura 13: Amenazas a las redes y sistemas de información

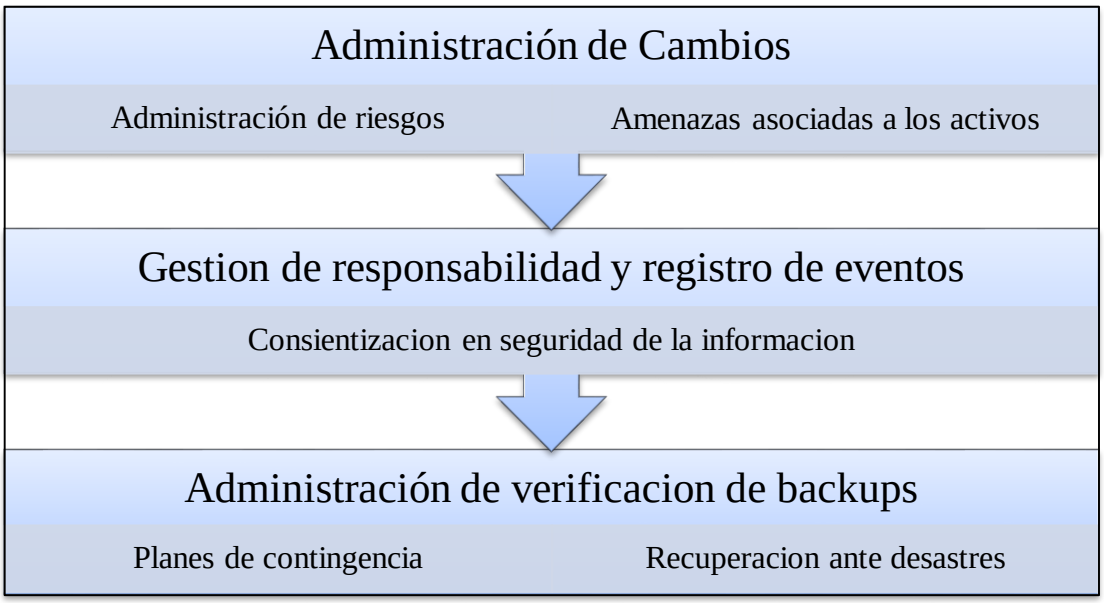


Fuente: Sistemas de información autor: Javier Areitio

d) Medidas de Protección

Después de reconocer los elementos que se desea cuidar, así como las posibles fallas y agujeros a las que nos podemos exponer y los viables atacantes que pretenden violar la seguridad de la empresa del grupo SUEZ ha de estudiar la forma de proteger los sistemas, sin brindar aun ejecuciones específicas para resguardar, ya que no constituirán reglas, sino componentes.

Figura 14: Procesos principales de la administración



Fuente: Sistemas de información autor: Javier Areitio

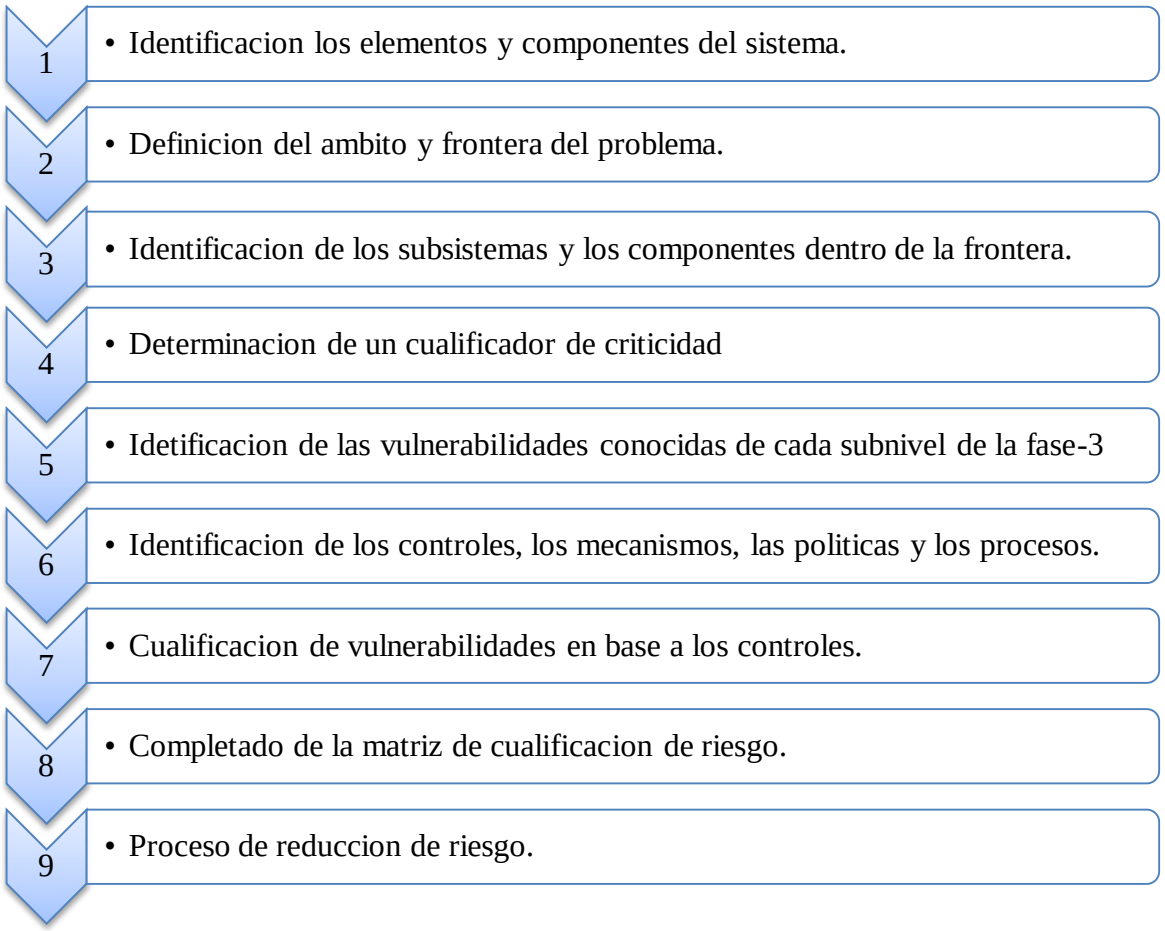
e) Control de Riesgos

La tarea de riesgos de seguridad puede definirse como el paso de igualar, medir, controlar y reducir los riesgos de seguridad en la red en el grupo SUEZ, a un nivel conforme al valor de los activos salvaguardados. La seguridad no solo debe verse como una inversión que permite aumentar la productividad, sino que es un elemento clave en la continuidad de los negocios. La concepción de la seguridad, solo como un gasto, ha quedado, desde hace mucho tiempo obsoleto.

f) Fases del proceso de reducción de riesgos seguridad

La gestión de riesgos puede utilizarse durante diferentes fases, como la pre adquisición, el diseño de arquitectura, y otras fases de la evaluación del sistema para establecer el nivel de riesgo. Existen nueve fases.

Figura 15: Estudio de peligros de seguridad

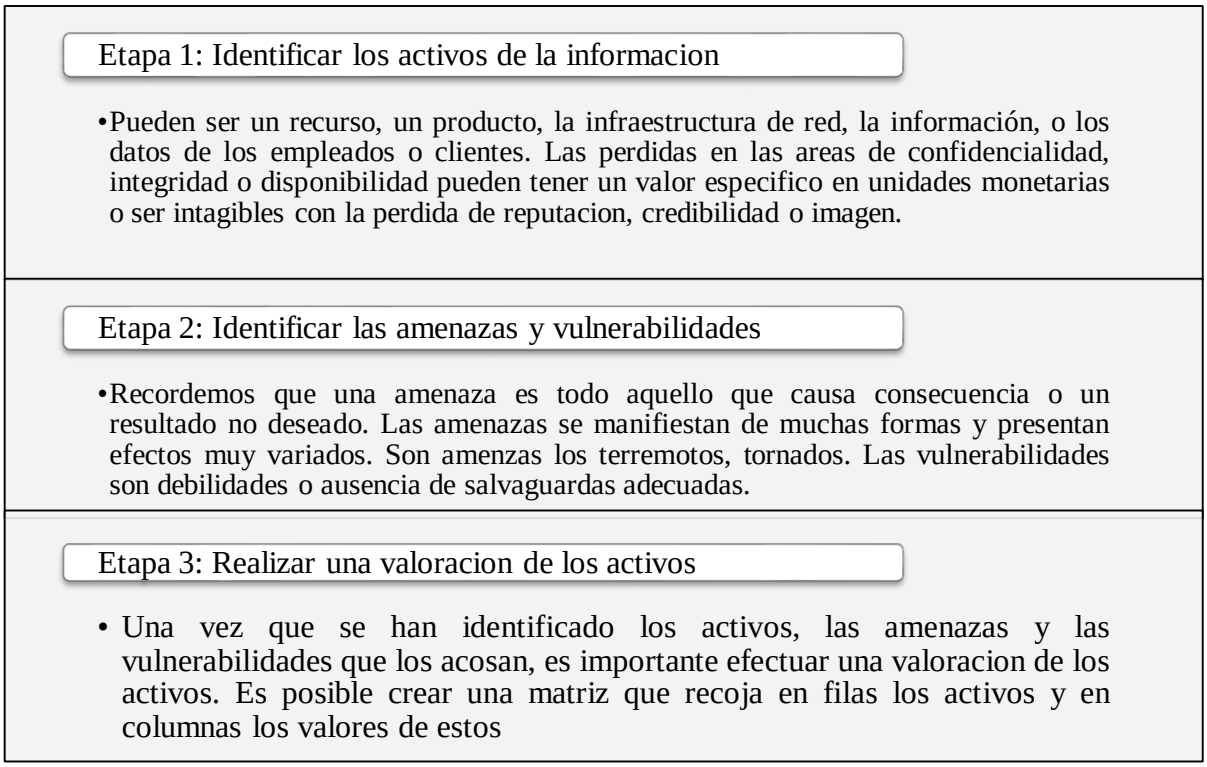


Fuente: Redes, informática autor: Javier Areitio

g) Fases para Determinar el ROI (retorno de inversión) en el Grupo SUEZ.

Para determinar el retorno de inversión o ROI (Return on investment) en seguridad o ROSI (Return on Security Investment) se pueden seguir las siguientes etapas.

Figura 16: Fases para determinar retorno de inversión



Fuente: Sistemas de información autor: Javier Areitio

1.3.5.3 CONTROL DE ACCESO: AUTENTIFICACIÓN, AUTORIZACIÓN Y CUMPLIMIENTO

El control de acceso es una expresión genérica utilizada para elegir el proceso por el que un sistema de red o software o monitor de referencia controla la interacción entre los usuarios y los elementos del sistema, de tal modo que los primeros que accedan a los recursos deseados. El control de acceso permite implementar una política de seguridad, que está establecida por las insuficiencias de la empresa y las normas corporativas. Estas necesidades incluyen la confidencialidad, integridad, disponibilidad, accesibilidad y el no repudio.

a) Control Acceso

Los elementos del control de acceso son los siguientes:

- Sujetos y principales: Son las entidades activas de un sistema de red o computación. Los sujetos son los usuarios o los intrusos. Se suele suponer que un sujeto es sinónimo de usuario. Un principal, atributo o propiedad asociada.
- Objetos: Son entidades pasivas o recursos de un sistema de computación, como son los ficheros, los directorios, carpetas o impresoras.

b) Control de Acceso y Modelos de Seguridad

En el ámbito de los sistemas de red e información, se relaciona con muchos y diferentes tipos de recursos. Esto requiere un conjunto complejo de operaciones y actividades a realizar, que pueden ser de naturaleza operacional u orientada a la gestión. El control de acceso debe estar dentro del contexto de una política de seguridad apropiada a las diferentes aplicaciones y las características del sistema.

Al clasificar los modelos de seguridad nos encontramos con dos grandes categorías diferentes, el control de acceso y el flujo de información, que controla los datos transmitidos en la red.

c) Operaciones de Acceso

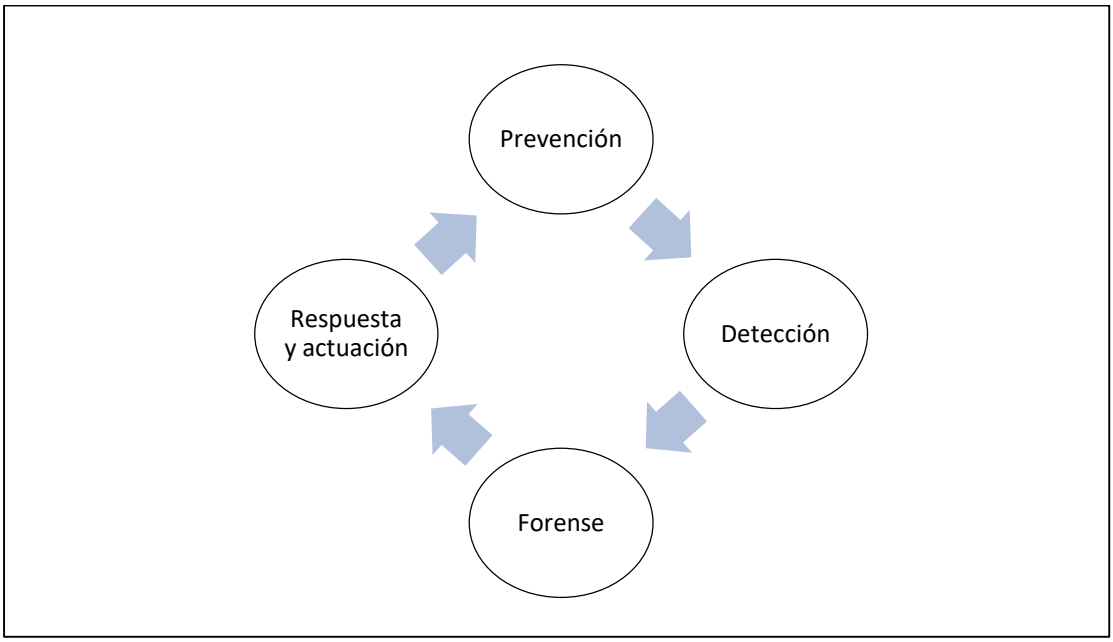
Las operaciones de acceso son las interacciones entre un objeto y un sujeto. En un sistema operativo multiusuario, los usuarios tienen acceso para abrir determinados ficheros. Los archivos se abren para leer o escribir, de modo que el sistema operativo puede evitar conflictos cuando 2 usuarios tratan de escribir simultáneamente sobre el mismo archivo

d) Los 4 enfoques de Seguridad

A la hora de abordar la seguridad global de cualquier tipo de sistema de red de una organización se puede los siguientes enfoques.

- **Prevención:** Para evitar un problema de seguridad, en primer lugar, se eliminan las vulnerabilidades y amenazas, se reduce la visibilidad del recurso de cara al exterior-
- **Detección:** Se comparan los riesgos considerados aceptables por las directrices de política de seguridad de la organización con las acciones que se observan, y se ejecuta un proceso de notificación para el personal.
- **Respuesta y actuación:** Consiste en responder a una brecha detectada, de una forma que concuerde con las directrices de la organización. La respuesta puede ser reactiva ante alguna acción que se haya producido, o proactiva, anticipándose a cualquier fallo que puede suceder.

Figura 17: Cuatro enfoques de seguridad en la red del Grupo SUEZ

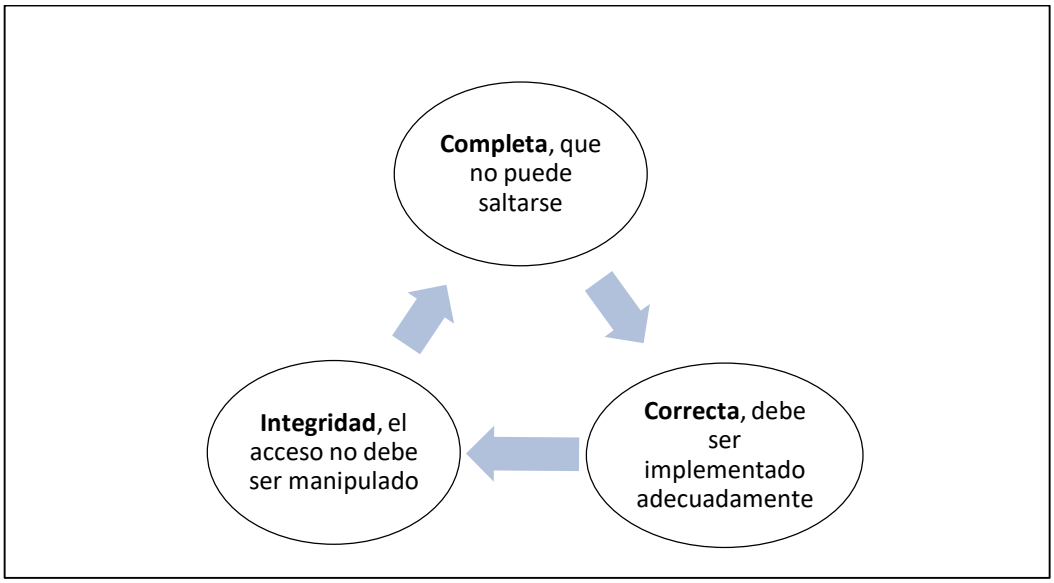


Fuente: Sistemas de información autor: Javier Areitio

e) Políticas de Control de Acceso

Una regla de control se puede contemplar desde diversos puntos, ejemplo, puede precisar como un acumulado de reglas que definen las condiciones bajo las que los iniciadores pueden acceder a los objetivos. También, puede especificarse como un agregado de leyes, reglas y prácticas que regulan la forma que el grupo SUEZ. Gestiona, protege y distribuye información que tiene cierto nivel de sensibilidad o riesgo. Asimismo, puede verse como un agregado de filtros, procesos y instrucciones para delimitar el uso de los servicios de TI, que pueden ser programas o procesos o aplicaciones autorizadas en la red. Estos procedimientos introducen restricciones que controlan el acceso a la red de un sujeto a un objeto o impiden el uso no autorizado de un recurso.

Figura 18: Características de la Política de Control de Acceso



Fuente: Sistemas de información autor: Javier Areitio

f) Administración de Control de Acceso

La efectividad del mecanismo del control de acceso depende, casi por completo, de la precisión y de la confianza en la información utilizada en la toma de medidas de control de acceso. Debe tener sumo cuidado para asegurar que la información que describe la política de control de acceso solo puede generarse o revisarse por un individuo autorizado. Esta información estará sujeta, por tanto, a la propia política y al propio mecanismo de protección de control de acceso, a un nivel incluso más sensible que los objetivos protegidos por estos mecanismos.

1.4 Formulación del Problema

1.4.1 Problema Principal

¿Cuál es la relación entre el modelo de seguridad y el control del tráfico en la red LAN, basado en la ISO/IEC 27002:2013 en Grupo SUEZ?

1.4.2 Problema Secundario

¿Cuál sería el efecto del modelo de seguridad en la disponibilidad de la información, en el Grupo SUEZ?

¿Cuál sería el efecto del modelo de seguridad en las solicitudes webs (internet), en el Grupo SUEZ?

1.5 Justificación del Estudio

1.5.1 Justificación Tecnológica

El mundo digital de la información está avanzando a pasos muy rápidos en la construcción de software y hardware que integran diversas funciones para la prevención de la información, uso adecuado de los servicios de la red y gestión de ancho banda de internet. Por otro lado, existe una inseguridad en la transferencia de información por internet, y a nivel de empresas existe el acceso no autorizado a información confidencial, divulgación de datos personales, robo de información, negativa de ingreso a servidores, acceso no acreditado a recursos y servicios, y cambio de información, por estas razones, el presente proyecto de investigación tiene como propósito desarrollar un modelo de seguridad en Linux a fin de proteger la información privada, imagen y reputación del grupo industrial SUEZ y estar alineados a los retos actuales que la tecnología informática.

En este proyecto de investigación se utilizara el Software Linux en la distribución Centos, dado que brinda opciones para proteger a la red a nivel perimetral del grupo industrial SUEZ, es decir conexiones externas no autorizadas desde internet que intenten acceder a la información de la empresa. Linux también es un gestor de accesos a páginas web, es decir deniega o permite el acceso a las páginas web de internet.

1.5.2 Justificación Institucional

Actualmente hay una preocupación de la gerencia general del Grupo SUEZ, ya que la infraestructura de comunicaciones de red no tiene un sistema de que proteja la información frente algún ataque cibernético que pudiera recibir desde redes externas (internet), esta amenaza puede directamente a las áreas de finanzas, comercial e ingeniería dado que son la áreas más críticas que manejan la información financiera como; los planes de proyecto de clientes, la planificación estratégica de la empresa, propuestas de ingeniería de los futuros proyectos y propuestas económicas para ser presentado a los clientes, tampoco los procesos de las áreas del grupo Suez están alineados a controles de seguridad de ninguna norma técnica lo que coloca a la red en un punto vulnerable.

El problema es debido que la red de comunicaciones no está protegida, lo que ocasionaría que los servicios de TI se podrían paralizar causando un malestar del personal por la acumulación de trabajos, por lo que tendrían que quedarse más horas/días y que la empresa tendría que cubrir la alimentación y movilidad del personal generando costos adicionales a la compañía.

La presente tesis de estudio propone un método de protección de intrusos con mecanismos de seguridad y control con Linux que permitirá proteger la información que es el activo más meritorio de la organización, esta propuesta de proyecto dará las recomendaciones para la diligencia de mecanismos de acceso y a los servicios de tecnologías y a la información. De esta manera se reducirá las molestias de los empleados hacia el área de TI. Con la implementación del proyecto de investigación los procesos administrativos y tecnológicos tendrán mayor fluidez. El resultado de esta investigación se aplicara en el grupo industrial SUEZ, no obstante las funcionalidades del sistema de protección de intrusos (IPS) es aplicable en otras empresas, pymes y empresas privadas. Finalmente los hogares del Perú serán la más beneficiada con el impacto positivo que causara consecuencia de este proyecto, ya que el soporte tecnológico al proyecto de tratamiento de agua y desagüe que tiene a cargo el grupo SUEZ en distintos lugares del Perú.

1.5.3 Justificación Operativa

Esta tesis solucionara los siguientes problemas: perdida de información, divulgación de información confidencial, bloqueo de acceso a servidores, acceso no autorizado a recursos y servicios, ataque de denegación de servicios y ataques cibernéticos trayendo como consecuencia pérdida de tiempo en recuperar la información, restaurar los servicios generando costos a la empresa y afectando la imagen corporativa del grupo SUEZ.

También se justifica dado que el nivel operativo es de mi dominio y conocimiento técnico, conozco la problemática que actualmente tiene el grupo industrial SUEZ, por esta razón podría ser valorado y tomado en cuenta. Uno de los aportes principales es desarrollar un sistema perimetral de red para salvaguardar la información y los elementos de red de la empresa frente a los ataques cibernéticos, lo que permitirá una continuidad de los procesos y operaciones del área de ingeniería, finanzas y sistemas.

Con un software de seguridad en Linux se aplicara los mecanismos de protección y prácticas de controles de seguridad basado en la norma técnica ISO/IEC 27002:2013 reduciendo el tiempo en la resolución de fallas de red (troubleshooting), es decir la detección de la causa raíz de un problema que tenga un impacto negativo que afecte la continuidad de los procesos de la empresa. Los servicios de red no se interrumpirán dado que el desarrollo del sistema de protección será elaborado teniendo en cuenta una metodología y recomendaciones técnicas de expertos en Linux.

Esta investigación brinda las recomendaciones y aportes técnicos. Operativamente esta investigación se justifica dado que propone una capa de seguridad entre la red externa y la red interna para salvaguardar la información y los elementos de red del grupo industrial SUEZ ante una amenaza externa que pudiera sufrir. Por tanto, los beneficios que se puede resaltar de este proyecto al contar con una capa de seguridad con mecanismos de seguridad, control y alta velocidad para los servicios y sistemas de tecnologías de la información serán más eficientes por consiguiente las operaciones financieros y administrativos de los empleados no se detendrán.

1.5.4 Justificación Económica

La influencia de estas pérdidas para el año 2019 lograría aumentar en el 4to y 5to veces más si las compañías no identifican esta inminencia cibernética y retan por la prevención, y en forma suplementaria, por un amparo financiera. Es un asunto muy complejo cuando se toma en cuenta que las organizaciones tardan aproximadamente 57 días en reprender los resultados de un ataque y gastan una media de $ 32,000 por día.

La seguridad digital de las empresas públicas, compañías privadas y las personas es un argumento que ha empañado gran relevancia en el continente, y que se ha aumentado durante el actual trimestre del año en el que centenas de usuarios y empresas experimentaron dos ataques de gran escala. Según un reciente estudio de Forbes, para el 2019 la ola del ciberataque en el mundo alcanzará los US$ 2.1 billones.

En américa, las males económicas fruto de este tipo de amenazas ascienden a US$ 76,766 millones. Entre los países mayor afectados se encuentra Brasil, con US$ 19,291 millones en pérdidas; seguido por México (US$ 11,921 millones), Venezuela (US$ 9,142 millones) y Argentina (US$ 7,400 millones).

Nuestro país (Perú) se encuentra en el 7mo posición entre los países más afectados por el ciberataque en la región, reconociendo pérdidas que llegan los US$ 4,782 millones para el cierre del 2017. Según el diario Gestión para los siguientes 3 años Perú registrara U$$ 4,782 millones en pérdidas por delitos cibernéticos (redacción gestión 10.08.2017 – 06:56PM)
Era preciso puntualizar los antecedentes para dar a conocer las grandes cantidades de dinero que se pierda al no contar con mallas de seguridad perimetral en una red de comunicaciones como un sistema de prevención de ataques cibernéticos. Por consiguiente, la presente tesis de estudio se justifica económicamente dado que los recursos que serán utilizados en su implementación son: PC que será el servidor, software Linux en la distribución de Centos, 2 tarjetas de red, 2 cables UTP, 01 switch de red en capa 2 no generando mayores gastos al Grupo SUEZ, no obstante como retorno de inversiones trae consigo muchos beneficios técnicos y ahorro de dinero.
Por tanto, el progreso y la implementación del presente tesis de estudio se justifica económicamente dado no generara gastos mayores al Grupo SUEZ.

1.6 Hipótesis

1.6.1 Hipótesis General

"El modelo de seguridad tendrá un efecto positivo en el control del tráfico de la red LAN basado en la norma ISO/IEC 27002:2013, en el Grupo SUEZ.".

1.6.2 Hipótesis Específica

El modelo de seguridad tendrá un efecto positivo en la disponibilidad de la información, en el Grupo SUEZ.

El modelo de seguridad mejorara las solicitudes web, en el Grupo SUEZ.

1.7 Objetivo

1.7.1 Objetivo General

Determinar el efecto del modelo de seguridad y el control del tráfico en la red LAN, basado en la ISO/IEC 27002:2013 en Grupo SUEZ.

1.7.2 Objetivo Específico

Determinar el efecto del modelo de seguridad en la disponibilidad de la información, en el Grupo SUEZ.

Determinar el efecto del modelo de seguridad en las solicitudes webs (internet), en el Grupo SUEZ.

II. MÉTODO

2.1 Diseño de Investigación

2.1.1 Tipo de Estudio

La tesis de tipo aplicado investiga el conocer para crear, proceder y construir. (Martínez, 2007). Afirma. "Con el propósito de poner en habilidad los instrucciones obtenidos a una realidad concreta y convertir hasta donde sea posible optimar". (p.21)

"Tomando como referencia la definición anterior, la presente investigación":

Aplicada – Experimental

2.1.2 Diseño de Estudio

El diseño de tipo pre-experimental busca aplicar una cierta incitación o método a un grupo y luego aplicar una medición de una o más variables para mirar cuál es el nivel del grupo en éstas. Hernández (2009) afirma:

Según lo mencionado, "el diseño del presente proyecto de investigación es Pre – experimental ya que realizara una medición de los indicadores en dos momentos, tanto en el pre-test como en el post-test, y se hará una asimilación entre los consecuencias logrados, estas pruebas se realizaran en una maqueta (prototipo) teniendo en cuenta los indicadores".

2.2 VARIABLES, OPERACIONALIZACIÓN

2.2.1 DEFINICIÓN CONCEPTUAL

a) Modelo de Seguridad de redes

(GOMEZ, Álvaro, 2007, Págs. 401-402). Es un sistema que permite prevenir las intrusiones neutralizando las acciones de su ataque. Un proxy funciona por medio de reglas que establece estrategias de seguridad para resguardar la red de una agresión informático. Según su base datos de firmas un ataque puede ser neutralizado en tiempo corto o progresar las acciones de su agresión.

b) Seguridad de la Información ISO27002

(López & Quezada, 2016, p. 26). La ISO 27002 viene a ser una norma, la cual llega a estar en constante avance, de acuerdo a la tecnología. El objetivo principal de la seguridad de la información es que las empresas puedan cumplir con su misión con todo lo que tienen

implementado, de diferentes métodos que aporten con el cuidado y el estudio de riesgos, incidentes o vulnerabilidades de la información tanto de la organización como de sus clientes. El término seguridad de la información integra 3 dimensiones: disponibilidad, integridad y confiabilidad que dan un vinculado de medidas defensoras y reavivas de las compañías y de los elementos de TI para salvar y cuidar la información.

2.2.2 DEFINICIÓN OPERACIONAL

a) Solicitudes Web (Internet)

(Alejandro Mora, 2008). Un modelo de seguridad con proxy server a nivel operacional identifica, clasifica y detiene con exactitud el tráfico inusual, por ejemplo adware y virus de redes, uso alto de aplicaciones antes de que afecten la flexibilidad de una organización. Proporcionan una protección contra amenazas externas con una exclusiva unión, colaboración en toda la red.

b) Seguridad de la Información ISO27002

Esta norma fue publicada en el año 2000 y convertido al español en 2006; es un acumulado de normas no certificables que facilitan un marco de administración de la Seguridad de Información, adaptable a cualquier empresa.

La norma define líneas principales para iniciar, efectuar, conservar y optimizar la gestión de la seguridad de la información. Los propósitos indicados en esta norma ofrecen una guía universal sobre los objetivos aceptadas usualmente para la administración de la seguridad de la información.

2.2.3 METODO DE ANÁLISIS DE UN SISTEMA DE PROTECCION DE INTRUSOS

a) Análisis en profundidad

(Javier Areitio, 2008. Pag. 190). El sistema de prevención de intrusiones de detecta y bloquea los intentos de intrusión, la transmisión de código malicioso y las amenazas procedentes de la red externas, sin que ello impresione al performance de la red del Grupo SUEZ.

Estos pueden tomar operaciones determinadas sobre los paquetes monitoreados, como frenar su paso, es decir siendo reactivos más no indiferentes frente a un incidente. De este modo, sus características se acercan más a la tecnología de los firewall, sin embargo

basando su estudio en la conducta del paquete, y no en la analogía puerto/protocolo de la comunicación.

Un servidor proxy dentro del análisis que realiza ante un ataque tiene las siguientes fases:

b) Preprocesadores

(Javier Areitio, 2008. Pag. 193). Los preprocesadores son plugins que admiten extender la funcionalidad del proxy para tratar los paquetes que vienen desde el decodificador, Se encargan de dar forma lógica a las tramas para poder descifrar la información de una manera mucho más fácil.

c) Aplicación de Reglas

(Javier Areitio, 2008. Pag. 193). Proxy utiliza algunos elementos entre los cuales son:

- frag3, stream4 y stream4_reassemble, flow, stream5, sfportscam, rpc_decode, ssh.

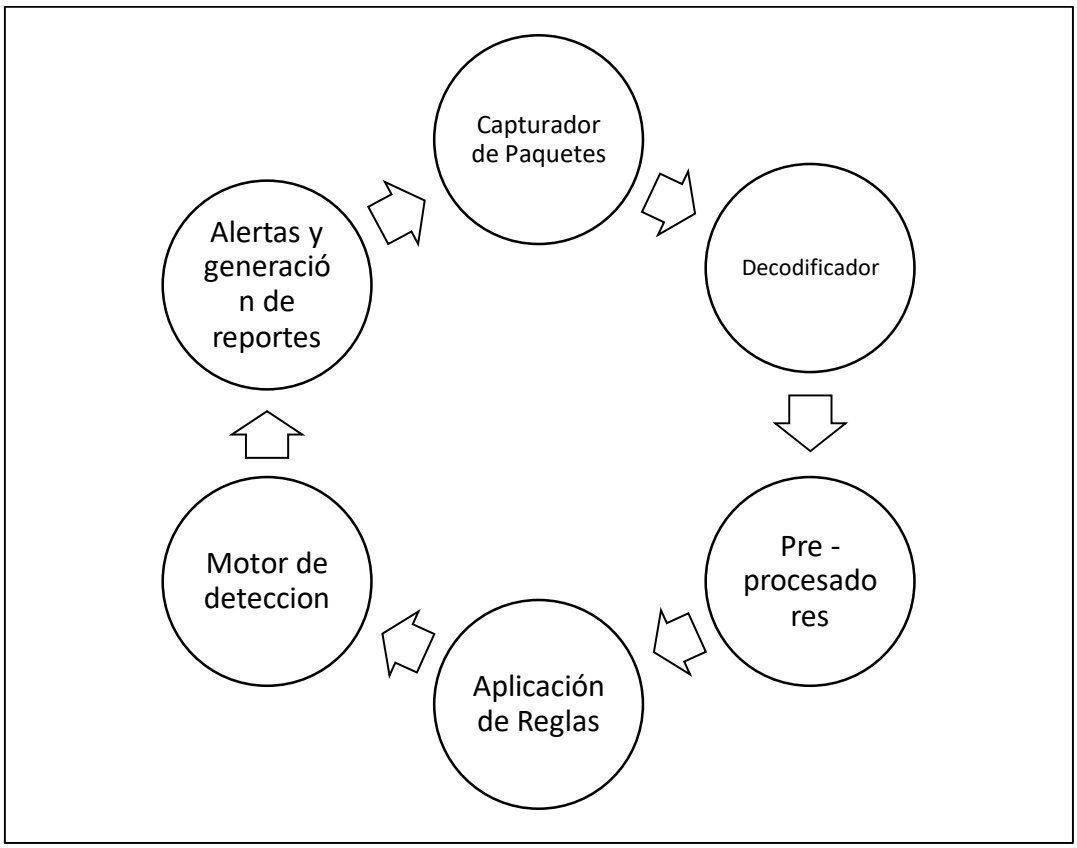
d) Motor de Detección

(Javier Areitio, 2008. Pag. 193). Es el responsable de descubrir si existe algún comportamiento malicioso dentro del paquete, esto se identifica haciendo una cotejo con las ACL previamente definidas y configuradas en las reglas, si existe una descubrimiento el motor ejecuta la criterio especificada para dicho incidente, luego la alerta pronunciada es guardado en un log, caso contradictorio al no existir una similitud con las ACL el motor lo retira.

e) Módulo de Salida / Reportes

(Javier Areitio, 2008. Pag. 194). Una vez estudiado la información por el motor de descubrimiento, es reportado la información ya sea en diferentes formatos y en distintos equipos.

Figura 19: Método de Análisis de un Servido Proxy

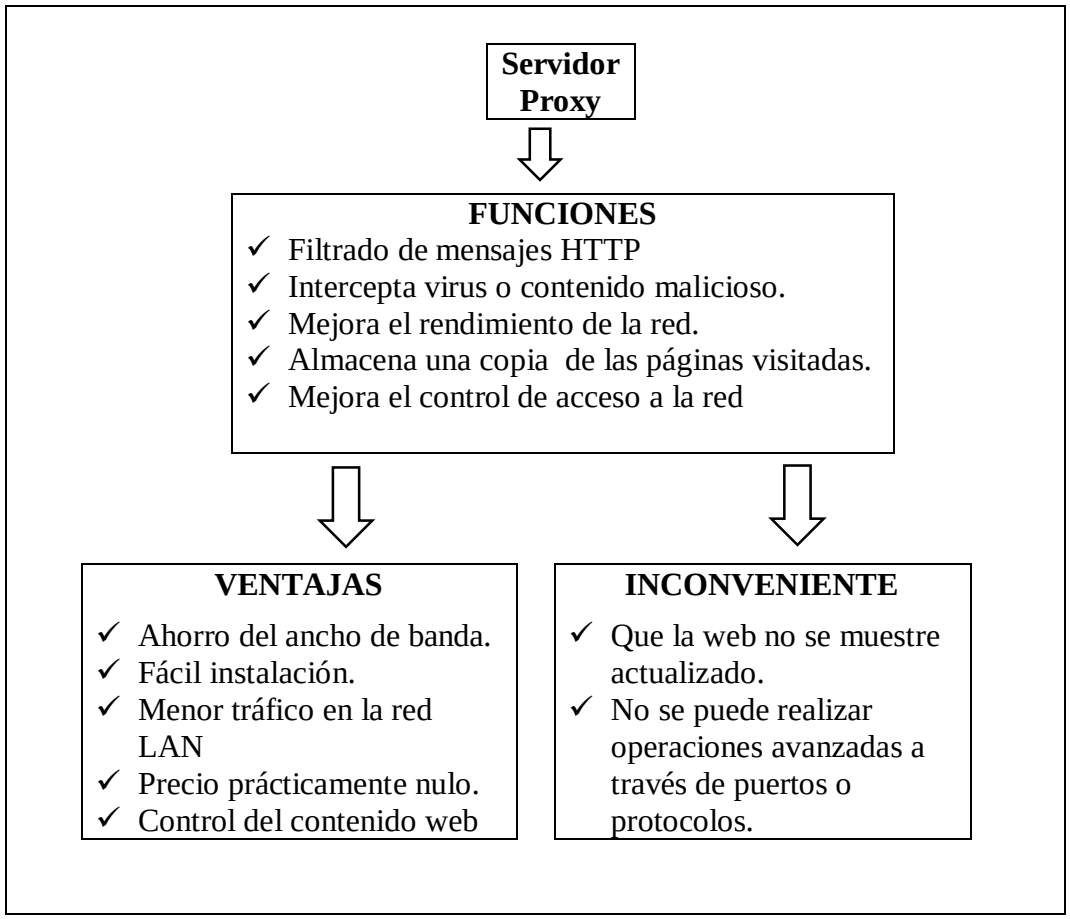


Fuente: Redes, informática y sistemas de información autor: Javier Areitio

f) Esquema de Funcionamiento de Sistema de Protección de Intrusos

En el esquema se muestra la forma de resguardar de intrusos manejando una combinación de técnicas de monitoreo, patrones, firmas y anomalías y heurísticas, análisis, valoración de vulnerabilidades, auditoria, generación de alarmas y acciones de defensa. El esquema muestra un modelo de administración de seguridad para áreas de redes medianas.

Figura 20: Esquema de Funcionamiento del Servidor Proxy



Fuente: Sistemas de información autor: Javier Areitio

g) Diseño de red del modelo de seguridad con servidor proxy

El diseño lógico del proxy se ha adecuado a la infraestructura actual del grupo SUEZ, teniendo en cuenta el equipamiento de servidores y switch de red de la empresa.

2.2.4 METODOLOGÍA PARA DESARROLLAR UNA POLÍTICA DE SEGURIDAD EN EL GRUPO SUEZ

a) Desarrollar una Política de Seguridad

(Javier Areitio, 2008. Pag. 110). Antes de abordar el paso de desarrollo de una política de seguridad conviene recordar algunas cuestiones clave como el hecho de comprender que la política de seguridad trata a los ataques a la seguridad de la información y especifica los procedimientos a adoptar en una organización para reducir la ocurrencia de un ataque y la reacción frente a la amenaza producida. Asimismo, se deben conocer los motivos para implantar una política de seguridad de la información, ya que forma el modelo del plan director de seguridad, asimismo como la importancia del desarrollo de una política y efectiva. Asimismo, las TIC están en constante evolución y traen nuevas y cambiantes amenazas que deben tener en cuenta.

b) Análisis y Valoración de Riesgo

(Javier Areitio, 2008. Pag. 110). La primera fase consiste en un exhaustivo análisis peligros de seguridad para nivelar la etapa en que se encuentra la seguridad dentro de la organización y proponer medidas de seguridad y controles para que se puedan efectuar los propósitos de negocio establecido. El primero fin de esta fase es identificar las amenazas a las que es susceptible la información de nuestra organización. Una vez hecho esto, deben estimar los riesgos asociados a cada una de ellas. El riesgo de que ocurra una amenaza se refiere al impacto de esta ocurrencia en los objetivos del negocio.

c) Construcción de la Política de Seguridad

(Javier Areitio, 2008. Pag. 110). Esta fase está relacionada con el desarrollo de la norma de seguridad, y se enfoca únicamente, en conocer los contenidos preparados de una política robusta, eficaz y eficiente. El documento que define la norma de seguridad de la información debe distribuirse a todos los usuarios del sistema. Debido a esto, la redacción utilizada para describir los procedimientos técnicos-organizativos o legislativos, deberá ser adecuada para permitir que todos los usuarios la entiendan adecuadamente

d) Implantación de la Política de Seguridad

(Javier Areitio, 2008. Pag. 111). Antes de implantar la norma de seguridad a todos los trabajadores, debe examinarse para no dejar ninguna laguna legal, también asegurar que

la norma es clara, breve y sólido. También, debe establecerse forma segura de la eficacia de la norma de seguridad que debe mostrar las leyes fijadas por ésta, para evitar obstáculos legales. Por otra parte, si un empleado despedido decide demandar a la empresa, un manuscrito de política de seguridad de la información sería la mejor ayuda para su defensa. La política de seguridad debe también tener en cuenta posibles implicaciones sociales y éticas.

e) Mantenimiento de la Política de Seguridad

(Javier Areitio, 2008. Pag. 111). Para que una empresa tenga un nivel alto de seguridad, su política de seguridad de la información debe desarrollar la identificación de nuevos tipos de ataques, por ello debe revisarse siempre. Si no, la regla dejara de ser utilizable. Esta fase es, posiblemente la más importante, en relación a la gestión de una norma efectiva de seguridad de la información a largo plazo. Esta fase supone un proceso continuo e implica revisiones permanentes y está ligada a la fase 1de análisis y valoración de riesgos. Por tanto, en caso de que sea necesario fedback de la política se debe seguir un conjunto de procedimientos para la implementación de dichos cambios para asegurar que se instituyen de manera adecuada y que no tengan repercusiones negativas debido a una política mal construida.

f) Implicación de todo el componente humano

(Javier Areitio, 2008. Pag. 120). El componente humano, engloba a todo tipo de personal desde el director, empleados, personal externo, visitas, clientes y socios corporativos. Todas las demás faces de las políticas están contenidas en esta fase. Aunque el desarrollo de la política es un proceso de gestión, mantenimiento de la misma necesita la colaboración de todos los empleados, observando las reglas establecidas en la política de seguridad. Uno de los factores más contribuyentes al fallo de una política es la falta de apoyo por parte de todos los empleados, ya que estos tienen que ser conscientes de que la seguridad de la información es de importante categoría para el propósito de llevar un negocio de forma competitiva, eficaz y eficiente. Si la dirección no muestra su apoyo a la política de seguridad propuesta, hay muchas posibilidades de que el resto de los trabajadores tampoco lo haga. Una falta de apoyo de los empleados da lugar a una política inútil y esto conlleva un plan o programa director seguridad muy pobre.

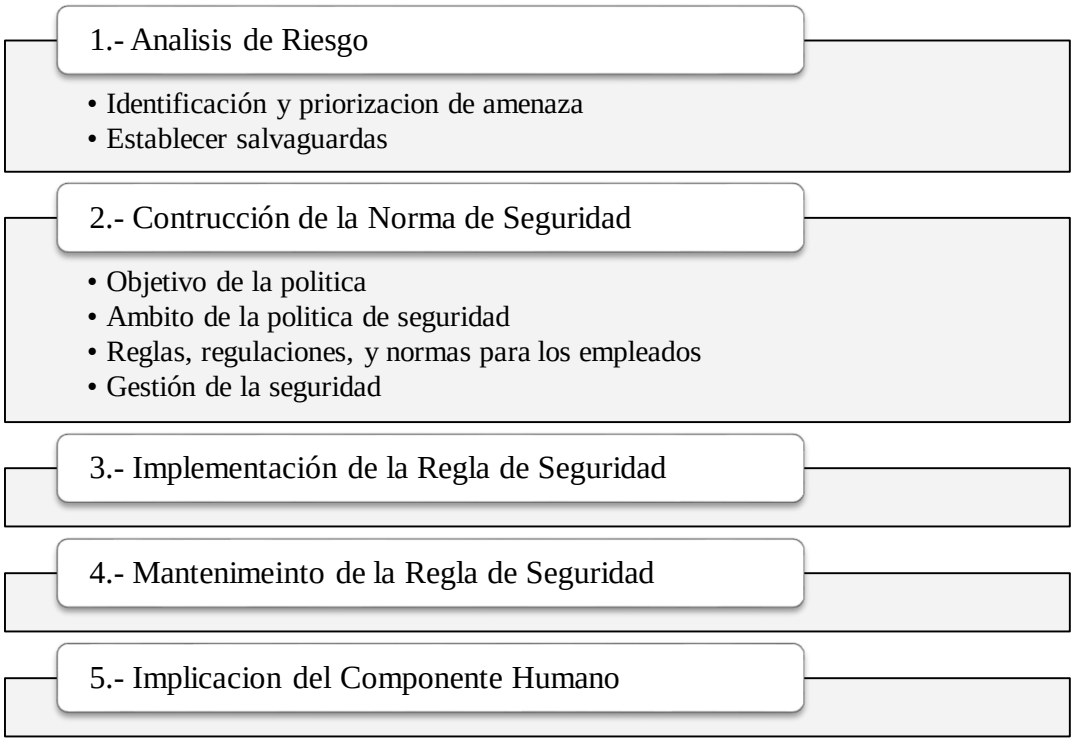
g) Causas del fallo de las políticas de seguridad

(Javier Areitio, 2008. Pag. 120). Entre las causas más habituales del fallo de una política de seguridad son:

- La falta de apoyo o soporte por parte de los empleados.
- Las implicaciones legales o económicas.
- Establecimiento de cuestiones disciplinarias a los empleados.

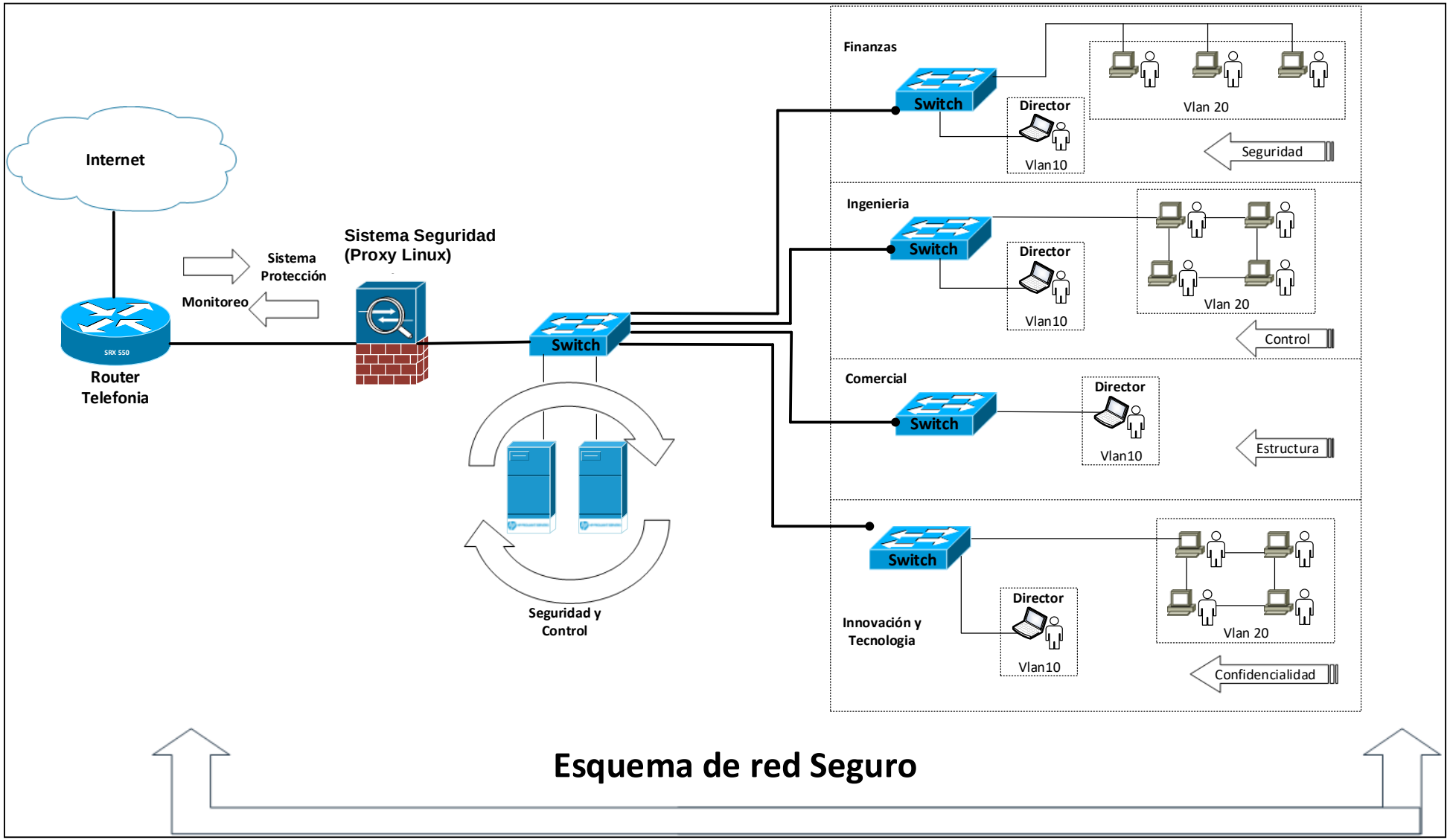
La política debe especificar qué información debe protegerse, quien tiene acceso a dicha información y auditar los accesos, y el grado de intensidad de seguridad que necesita los objetivos del negocio.

Figura 21: Metodología para desarrollar una política de seguridad



Fuente: Redes e informática autor: Javier Areitio

Figura 22: Propuesta de implementación del Modelo de Seguridad en Grupo Suez



Fuente: Elaboración propio

2.2.5 OPERACIONALIZACIÓN DE VARIABLES

La etapa de operacionalización de las variables permite detallar la funcionalidad, la distribución, las dimensiones y los indicadores de la variable de estudio.

Especificar dimensión disponibilidad VS N° de tickets.

La dimensión disponibilidad	Tiene un indicador cuantitativo que determinara el porcentaje o que tanto está disponible la información en la empresa, una información hace referencia a un aplicativo, una base datos, un email, entre otra información que alimente un proceso de negocio en la empresa.
N° de ticket.	Hace referencia a la cantidad de incidencias de red ocurridos, el cual es plasmado en un ticket de la mesa de ayuda. Asu vez, un numero de tickets es plasmado en un reporte de la mesa de ayuda, en ese sentido, para la presente investigación un reporte de la mesa de ayuda contenía muchos ticktes de incidencias.

Ejemplo.

Incidencia de red ➔ Ticket ➔ Reporte de la mesa de ayuda ➔ Disponibilidad de la información.

Teniendo en cuenta lo anterior, una incidencia de red afectaría directamente a la disponibilidad de la información, es por ello que el indicador de esta dimensión incluye al número de tickets de la mesa de ayuda. Por lo tanto en el análisis pre y post realizado se han notado diferencias en relación a la dimensión disponibilidad.

MATRIZ OPERACIONAL DE VARIABLES

Título: Modelo de Seguridad para el Control del Tráfico de Red LAN, basado en la ISO/IEC 27002:2013 en Grupo SUEZ

VARIABLES	DEFINICION CONCEPTUAL	DIMENSION	INDICADOR	DESCRIPCION	ESCALA DE MEDICION
INDEPENDIENTE Sistema de Seguridad.	**Sistema de Seguridad** (Javier Areitio, 2008) "Un modelo de seguridad está basado en resguardar archivos, base de datos y toda data importante. Está planteada para construir instrucciones y procesos que lleven a un inapreciable nivel de seguridad, idóneo de corregir todos los ataques. Hoy en día la red LAN cuenta con numerosos peligros de seguridad que se deben evaluar y mitigar".(Pag. 85) **Control de Trafico de red LAN** (GOMEZ, Álvaro, 2007, Págs. 401-402). Es el flujo de datos que se transmiten mediante un medio físico por la red. También, se puede decir que es una medida de la capacidad de transmisión de datos enunciada en kbps ó Mbps. Señala la capacidad teórica de una interconexión, sin embargo esta capacidad teórica se ve reducida por elementos perjudiciales tales como el retardo de transmisión, que pueden generar un deterioro en la eficiencia.	Disponibilidad	% de disponibilidad de la información. $D = \left(\frac{(1 - N°\ tickets) * 100\%}{Total\ de\ minutos\ al\ dia}\right) + 100\%$	La Disponibilidad de la información será medida con la cantidad de tickets de mesa de ayuda relacionadas a la lentitud de la red, entre el total de minutos al día.	Razón
DEPENDIENTE Control de Trafico de red LAN		Solicitudes Web	% de Solicitudes webs (internet) $W = \left(\frac{Cantidad\ de\ web\ bloquedas}{Total\ de\ web\ visitadas}\right) * 100\%$	Las solicitudes web serán medidas con la cantidad de páginas web bloqueadas entre el total de páginas web visitadas.	Razón

Título: Modelo de Seguridad para el Control del Tráfico de Red LAN, basado en la ISO/IEC 27002:2013 en Grupo SUEZ

2.2.6 INDICADORES

VARIABLES	DIMENSION	INDICADOR	DESCRIPCION	INSTRUMENTO
INDEPENDIENTE Sistema de Seguridad.	Disponibilidad	% de disponibilidad de la información $D = \left(\frac{(1 - N° \ tickets) * 100\%}{Total \ de \ minutos \ al \ dia}\right) + 100\%$	La Disponibilidad de la información será medida con la cantidad de tickets de mesa de ayuda relacionadas a la lentitud de la red, entre el total de minutos al día.	Ficha de registro.
DEPENDIENTE Control de Trafico de red LAN	Solicitudes Web	% de Solicitudes webs no autorizadas $W = \left(\frac{Cantidad \ de \ web \ bloquedas}{Total \ de \ web \ visitadas}\right) * 100\%$	Las solicitudes web serán medidas con la cantidad de páginas web bloqueadas entre el total de páginas web visitadas.	Ficha de registro.

MATRIZ DE CONSISTENCIA

Título: Modelo de Seguridad para el Control del Tráfico de Red LAN, basado en la ISO/IEC 27002:2013 en Grupo SUEZ

Problema General	Objetivos General	Hipótesis General	Variables	Dimensiones	Indicadores
¿Cuál es la relación entre el modelo de seguridad y el control del tráfico en la red LAN, basado en la ISO/IEC 27002:2013 en Grupo SUEZ?	Determinar el efecto del modelo de seguridad y el control del tráfico en la red LAN, basado en la ISO/IEC 27002:2013 en Grupo SUEZ.	El modelo de seguridad tendrá un efecto positivo en el control del tráfico de la red LAN basado en la norma ISO/IEC 27002:2013, en el Grupo SUEZ.	**INDEPENDIENTE** Modelo de Seguridad.	Disponibilidad Autor: Grupo SUEZ. Documento de contrato de servicio de internet. Pag. 47 Año: 2015	% de disponibilidad de la información $D = \left(\frac{(1 - N° \ tickets) * 100\%}{Total \ de \ minutos \ al \ dia}\right) + 100\%$
Específicos	**Específicos**	**Específicos**			
¿Cuál sería el efecto del modelo de seguridad en la disponibilidad de la información, en el Grupo SUEZ?	Determinar el efecto del modelo de seguridad en la disponibilidad de la información, en el Grupo SUEZ.	El modelo de seguridad tendrá un efecto positivo en la disponibilidad de la información, en el Grupo SUEZ.			
¿Cuál sería el efecto del modelo de seguridad en las solicitudes webs, en el Grupo SUEZ?	Determinar el efecto del modelo de seguridad en las solicitudes webs, en el Grupo SUEZ.	El modelo de seguridad mejorara las solicitudes web, en el Grupo SUEZ.	**DEPENDIENTE** Control de Tráfico de la Red LAN	Solicitudes webs Autor: Grupo SUEZ. Indicador elaborado por la empresa	% de Solicitudes webs no autorizadas $W = \left(\frac{Cantidad \ de \ web \ bloquedas}{Total \ de \ web \ visitadas}\right) * 100\%$

2.3 Población y muestra

2.3.1 Población

Levin & Rubin (1996), afirma: “Una población es un acumulado de todos los elementos que estamos estudiando, acerca de los cuales intentamos sacar conclusiones”. (p. 114)

La presente investigación, la población está conformada por 30 reportes de tickets de la mesa de ayuda registrados durante un mes.

2.3.2 Muestra

Según Muñoz Razo, Carlos (2011, p.117) “no siempre es posible hacer el levantamiento de los datos que conmueven un fenómeno, ni se pueden aprender todos los componentes del ámbito geográfico a los que se ajusta la tesis, ya que, además de inoperante, sería muy caro. Por ello, muchas veces se tiene que realizar un revolución parcial de la información, tomando una parte específica del universo de estudio.”

Según lo que señala el autor Muñoz Razo, para la presente tesis se usó como muestra el total de la población.

Cantidad de consultas.

La muestra está conformada por 30 consultas de mesa de ayuda realizadas durante un mes. Además, cabe mencionar que la suma de la muestra representa la totalidad de la población, por ello en la presente tesis se estudiará a toda la población.

2.3.3 Muestreo

Ortega 2009), señala: “El muestreo probabilístico es la posibilidad que tiene cada componente de la población de ser escogido para ser parte de la muestra. En esta tesis no se usará muestreo, ya que se aplicara el estudio estadístico sobre el total de la población para ambos indicadores”. (p. 205).

2.4 Técnicas e Instrumentos de Recolección de Datos, Validez y Confiabilidad

2.4.1 Técnicas de Recolección de Datos

2.4.1.1 Ficha de Registro

Hitoshi Kume (2002, p. 243). Las fichas de registro se diseñan considerando primero el propósito de la recolección de los datos y haciendo luego varias modificaciones creativas a fin de que los datos puedan recogerse y registrarse fácilmente y de manera adecuada al objetivo.

Carrasco Díaz (2007). "Las fichas de registro son una habilidad para la tesis social por excelentísimo debido a su uso, versatilidad, simplicidad y imparcialidad de los datos que con ella se obtiene". (p. 318)

Reportes	PRE-TEST		PRE-TEST	
	Cantidad de tickets	% Disponibilidad de la información	Cantidad de tickets	% Disponibilidad de la información
1	290	79.93%	10	99.38%

Cuadro: Matriz de contenido para análisis

2.4.2 Instrumentos de Recolección de Datos

2.4.2.1 Ficha de Registro

Según Kume (2002, p.11) "es un formato pre impreso en el cual surgen los ítems que se van a explorar, de modo que los datos puedan recogerse fácil y sucintamente".

Este instrumento es el que se ha manejado para la presente investigación.

2.4.3 Validez del Instrumento

Bernal (2010, p.247) menciona que "Un herramienta de cálculo legítimo cuando mide aquello para lo cual está propuesto. La validez señala que el grado con que logran deducir conclusiones a partir de los resultados logrados".

2.4.4 Confiabilidad

Fernández y Baptista (2006) nos dicen que: “La confiabilidad de un herramienta de medición se refiere al grado en que su uso repetida al mismo individuo u objeto produce resultados iguales”. (p. 277).

2.5 Método de Análisis de Datos

El método de análisis de datos a aplicar en esta tesis es de tipo cuantitativo, ya que la análisis es de tipo pre-experimental y se obtendrán datos estadísticas que logren ver si la hipótesis planteada en la tesis es correcta. Para el análisis de datos se utilizara la estadística inferencial, y se usará el software SPSS Statistics v.23 para el procesamiento de datos y generación de resultados estadísticos. Para las pruebas de pre-test y post- test se utilizara formas como la prueba de normalidad para saber el tipo de datos que se utilizó en la tesis.

2.6 Aspectos Éticos

Esta tesis concuerda a los aspectos éticos profesionales. Se ha respetado la veracidad de los resultados y de los datos suministrados por los usuarios del Grupo SUEZ, y respeta a los autores citados para proteger la presente tesis, nombrando en las referencias bibliográficas. Asimismo se ha mantenido en reserva la información confidencial a la que se ha podido tener acceso en la empresa.

III. RESULTADOS

3.1 Análisis Descriptivo

Se utilizó un aplicativo informático con el propósito de determinar el efecto de la disponibilidad de la información y cantidad de solicitudes web (internet) en el Grupo SUEZ, para ello se realizó un pretest que identificar las situaciones originarias de sus indicadores; luego se efectuó el modelo y de nuevo se registraron datos de sus indicadores. Los efectos descriptivos de estas medidas se indican en las tablas N° 6 y tabla N° 7.

Indicador: Porcentaje de Disponibilidad de la Información.

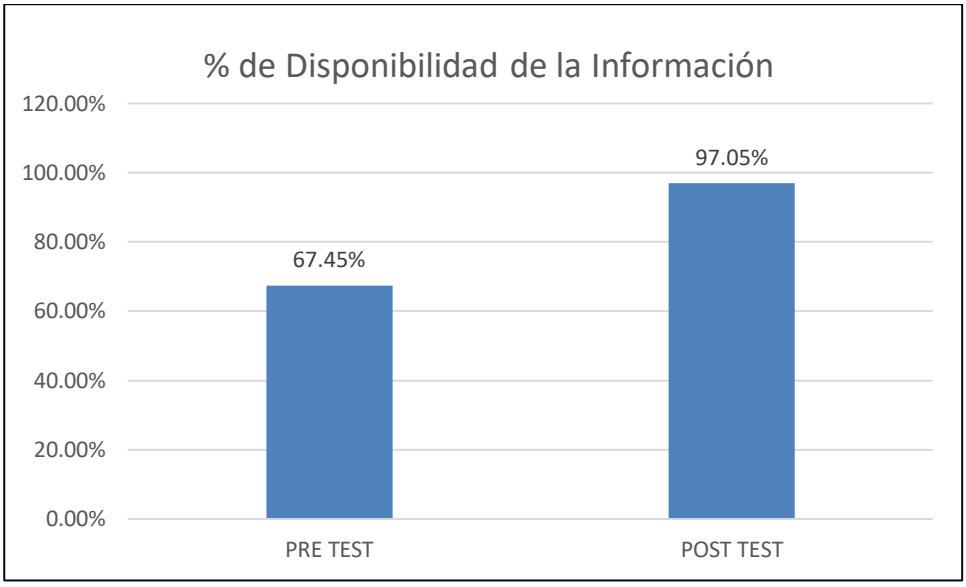
Tabla 4: Medida descriptiva del porcentaje de disponibilidad de la información antes y después de la implementación del modelo de seguridad.

	N				
	Válido	Perdidos	Media	Mínimo	Máximo
Pretest Porcentaje de disponibilidad de la información	30	0	67,4547	44,51	80,63
Postest Porcentaje de disponibilidad de la información	30	0	97,0537	93,75	99,72

Fuente: Propio (SPSS)

Para la investigación se consideró un porcentaje de disponibilidad de la información durante un mes (30 días), con relación a los datos adquiridos antes de la culminación del modelo de seguridad se halló una media de 67.45%, mientras que el resultado obtenido luego de la instalación del modelo de seguridad se encontró una media de 97,05%, esto señala una oposición importante antes y después de la implementación del modelo de seguridad para el Control del Tráfico de Red LAN en Grupo SUEZ, asimismo, el porcentaje mínimo de disponibilidad de la información fue de 44.51% antes y 93,05% después, claramente viendo un efecto positivo de la implementación del modelo de seguridad. (Ver figura N° 23)

Figura 23: % de disponibilidad de la información pre y post de la implementación del modelo de seguridad



Fuente: Propio (SPSS)

Indicador: Porcentaje de Solicitudes Webs (internet)

Tabla 5: Medida descriptiva del porcentaje de solicitudes webs antes y después de la implementación del modelo de seguridad.

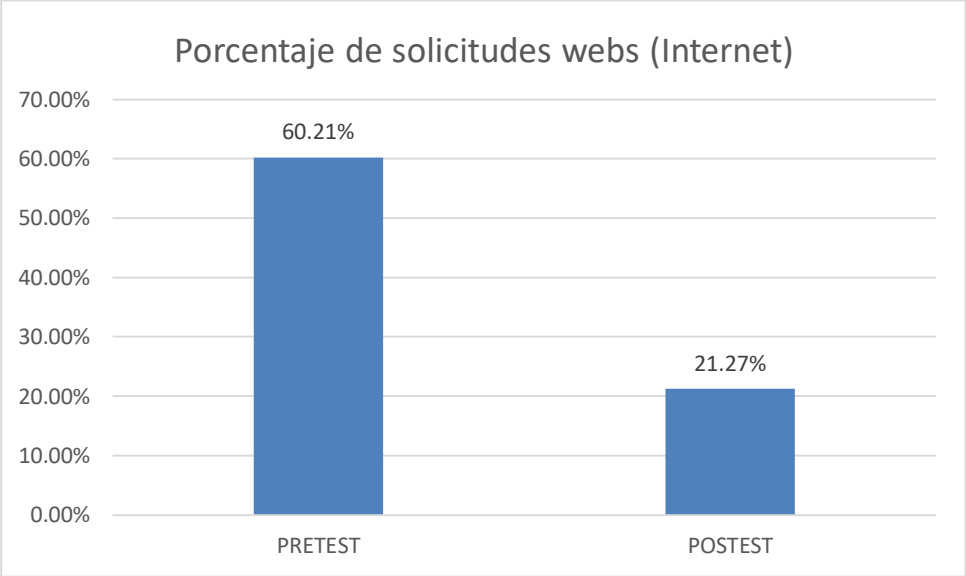
	N				
	Válido	Perdidos	Media	Mínimo	Máximo
Pretest - Porcentaje de solicitudes webs no autorizadas	30	0	60,2130	42,78	78,46
Postest - Porcentaje de solicitudes webs no autorizadas	30	0	21,2653	2,70	44,49

Fuente: Propio (SPSS)

En este investigación se consideró obtener el porcentaje de solicitudes web (internet) durante un mes (30 días), en comparación a los datos conseguidos antes de la ejecución del modelo de seguridad se halló una media de 60.21%, mientras que el resultado obtenido después de la implementación del modelo de seguridad se identificó una media de 21,26%, esto indica una discrepancia importante antes y después de la implementación del modelo de seguridad para el

control del tráfico de Red LAN en Grupo SUEZ, asimismo, el porcentaje mínimo de solicitudes web (internet) antes fue de 42.78% y 2,70% después, claramente viendo un efecto positivo de la implementación del modelo de seguridad. (Ver figura N° 24)

Figura 24: % de solicitudes web pre y post de la implementación
Del modelo de seguridad



Fuente: Propio (SPSS)

3.2 Análisis Inferencial

3.2.1 Prueba de Normalidad

Según Bernal (2014, p.20) menciona que "manejaremos la Prueba de Kolmogorov-Smirnov si hay más de 50 unidades de análisis o la de Shapiro-Wilk si hay menor a 50 unidades de análisis".

En ese sentido, para el presente estudio emplearemos la prueba de Shapiro-Wilk dado que la población es de 30 reportes de la mesa de ayuda durante un mes.

Indicador: Porcentaje de Disponibilidad de la Información.

Con el propósito de elegir la prueba de hipótesis, los datos fueron ingresados a la demostración de su distribución, solo si los datos de porcentaje de disponibilidad de la información tienen distribución normal. Para este estudio se utilizó la prueba de Shapiro –Wilk para 30 unidades de análisis.

Ho: Los datos tienen un comportamiento normal.

Ha: Los datos tienen no un comportamiento normal.

Tabla 6: Prueba de normalidad % de disponibilidad de la información antes y después de implementar el modelo de seguridad.

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Pretest Porcentaje de disponibilidad de la información	,859	30	,001
Postest Porcentaje de disponibilidad de la información	,936	30	,071

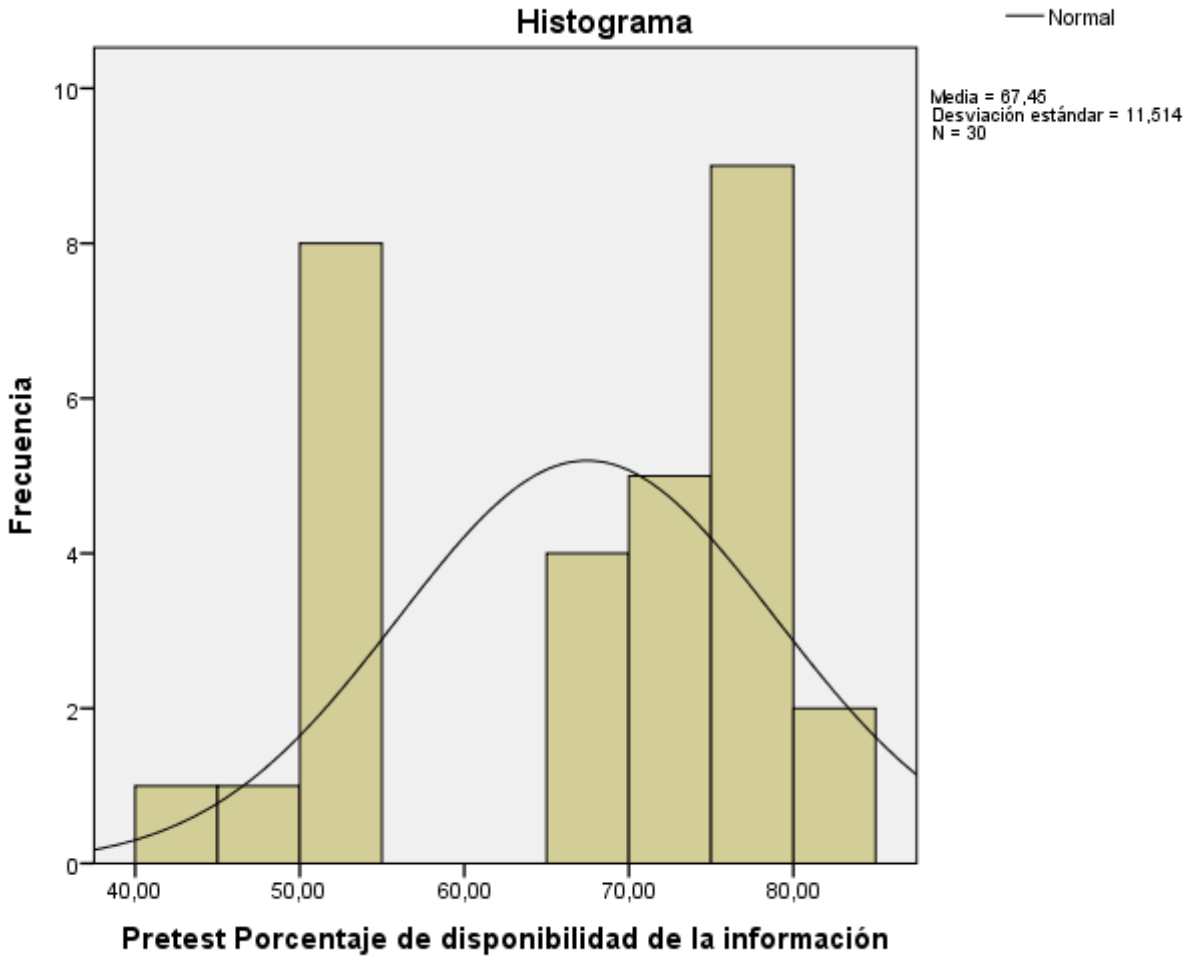
Fuente: SPSS (propio)

Los efectos del experimento muestran el grado de significancia de la muestra de % de disponibilidad de la información antes de implementar el modelo de seguridad fue de 0.01, cuyo valor es menor que el nivel de significancia 0.05, entonces la disposición es rechazar la hipótesis nula, en ese sentido los datos no siguen una distribución normal.

De igual modo, el resultado de la prueba indica que el nivel de significancia de la muestra del % de disponibilidad de la información posteriormente al implementar el modelo de seguridad es de 0.71, cuyo valor es mayor que el nivel de significancia 0.05, entonces la decisión es no rechazar la hipótesis nula, por tanto los datos no siguen una distribución normal.

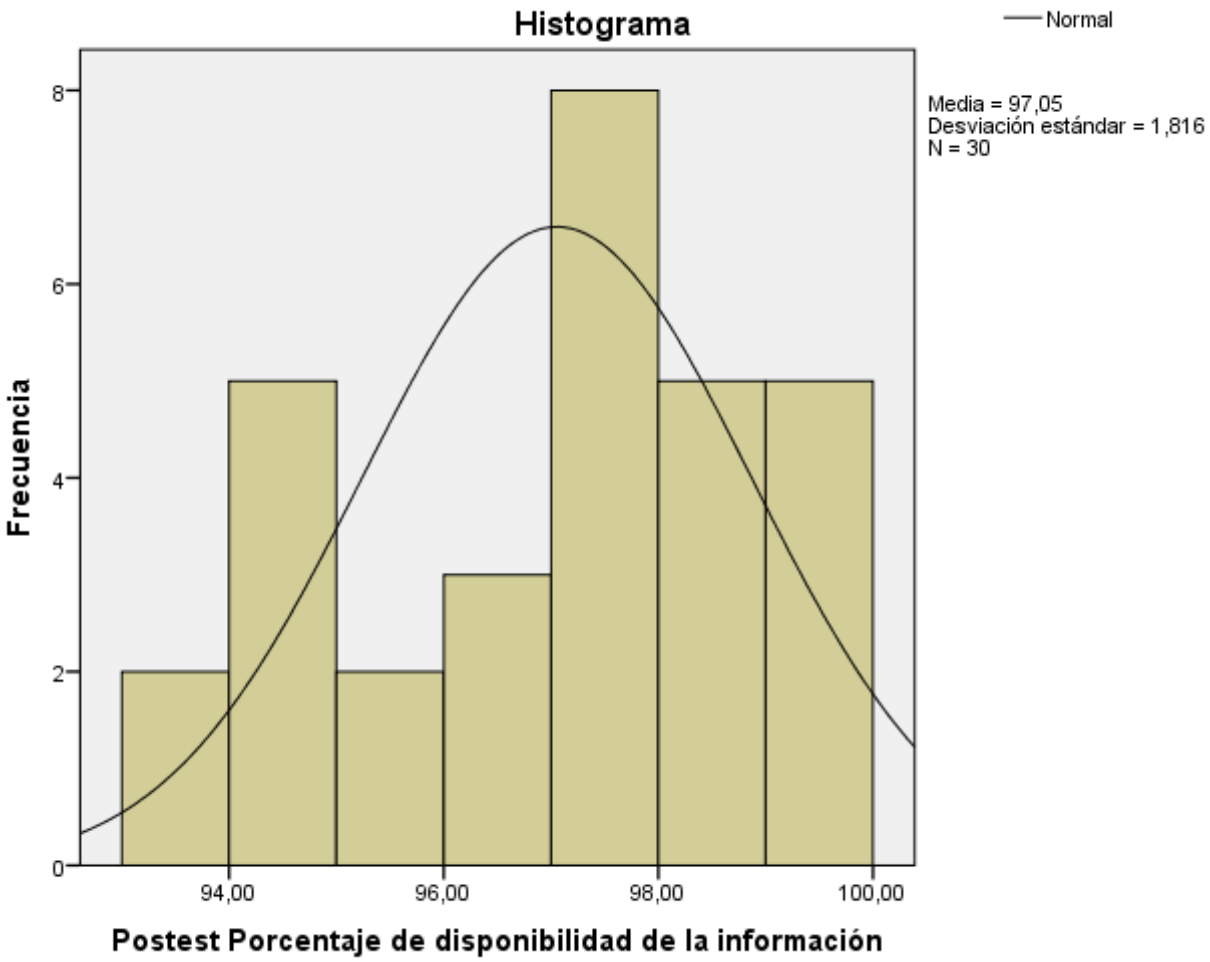
En la figura 25, se muestra un histograma de los valores conseguidos para el indicador "% de disponibilidad de la información" antes de implementar el modelo de seguridad en el Grupo Suez, obteniendo una media de 67. 45 en el valor porcentual. Asimismo, en el eje horizontal los valores de porcentaje de disponibilidad de la información, y en el eje vertical se puede verificar el número de veces que se representan los valores porcentuales en un intervalo, es decir, la frecuencia. Se puede apreciar como las barras no guarda proporción a la curva de distribución normal y esto es debido a que no existe distribución normal.

Figura 25: Prueba de Normalidad % de disponibilidad de la información antes de la implementación del modelo de seguridad



En la figura 26, se muestra un histograma de los valores logrados para el indicador "% de disponibilidad de la información" después de implementar el modelo de seguridad en el Grupo Suez, obteniendo una media de 97.05 en el valor porcentual. También, en el eje horizontal verificamos que los valores de porcentaje de disponibilidad de la información, y en el eje vertical se puede ver la cantidad de veces que representan los valores porcentuales en un intervalo, es decir, la frecuencia. Se puede apreciar como las barras no guarda proporción a la curva de distribución normal y esto es debido a que no existe distribución normal.

Figura 26: Prueba de Normalidad % de disponibilidad de la información después de la implementación del modelo de seguridad



Indicador: Porcentaje de Solicitudes Web (Internet)

Con el propósito de escoger la prueba de hipótesis, los datos fueron ingresados a la comprobación de su distribución, concretamente si los datos de solicitudes web (internet) contaban con distribución normal. Para este estudio se utilizó la prueba de Shapiro –Wilk para 30 unidades de análisis.

Ho: “Los datos tienen un comportamiento normal”.

Ha: “Los datos no tienen un comportamiento normal”.

Tabla 7: Prueba de normalidad dé % de solicitudes web antes y después de implementar el modelo de seguridad.

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Prestest - Porcentaje de solicitudes webs no autorizadas	,967	30	,469
Postest - Porcentaje de solicitudes webs no autorizadas	,917	30	,023

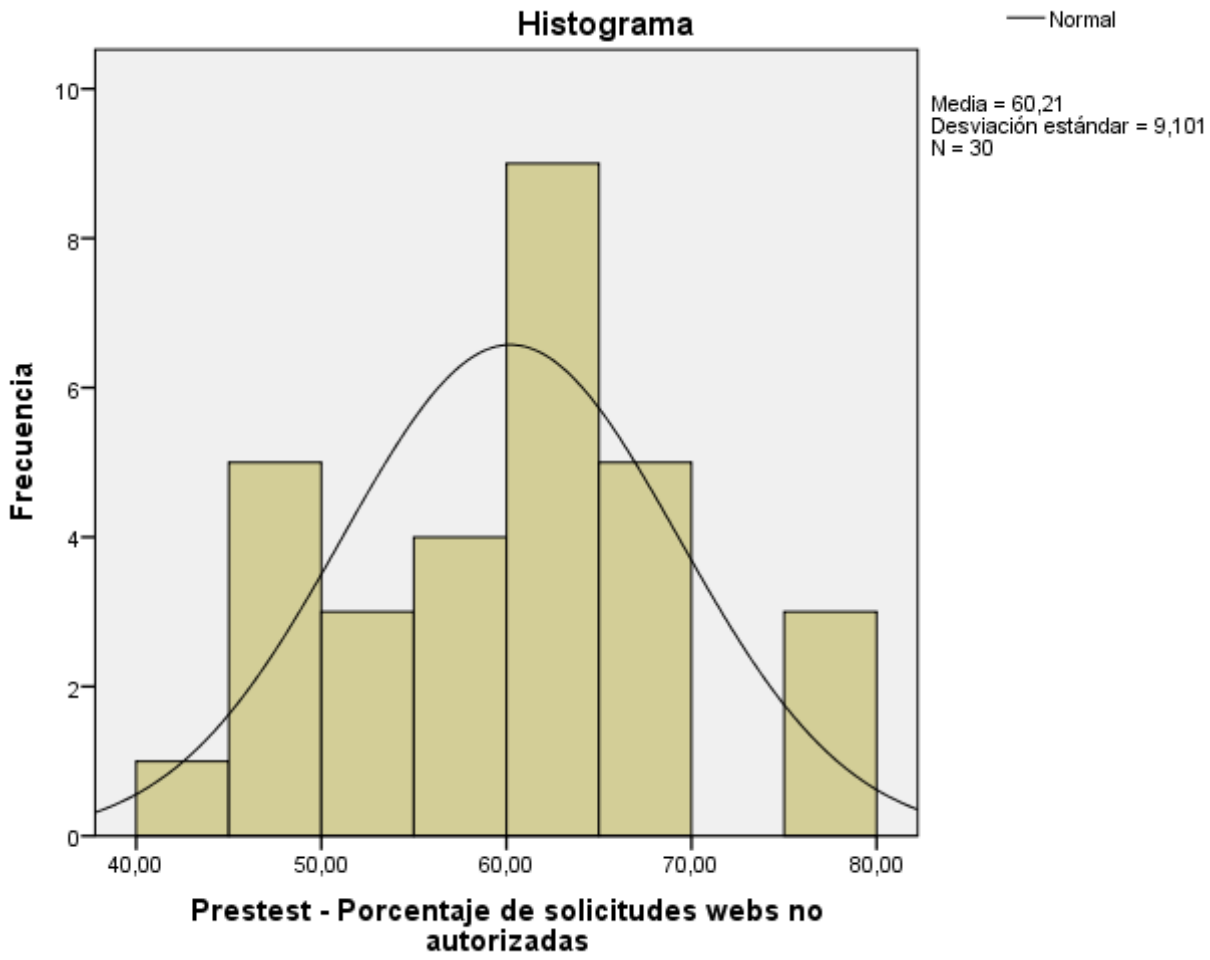
Fuente: SPSS (propio)

Los efectos del experimento señalan que el nivel de significancia de la muestra de % de solicitudes web (internet) antes de implementar el modelo de seguridad fue de 4.69, cuyo valor es mayor que el nivel de significancia 0.05, entonces la decisión es no rechazar la hipótesis nula, por tanto los datos no siguen una distribución normal.

De igual modo, el resultado de la prueba indica que el nivel de significancia de la muestra % de solicitudes web (internet) luego de implementar el modelo de seguridad es de 0.23, cuyo valor es menor que el nivel de significancia 0.05, entonces la decisión es rechazar la hipótesis nula, por tanto los datos no siguen una distribución normal.

En la figura 27, se muestra un histograma de los valores obtenidos para el indicador "% solicitudes web (internet)" antes de implementar el modelo de seguridad en el Grupo Suez, obteniendo una media de 60.21 en el valor porcentual. Igualmente, en el eje horizontal observamos los valores de porcentaje de solicitudes web, y en el eje vertical se puede ver el número de veces que se representan los valores porcentuales en un intervalo, es decir, la frecuencia. Se puede apreciar como las barras no guarda proporción a la curva de distribución normal y esto es debido a que no existe distribución normal.

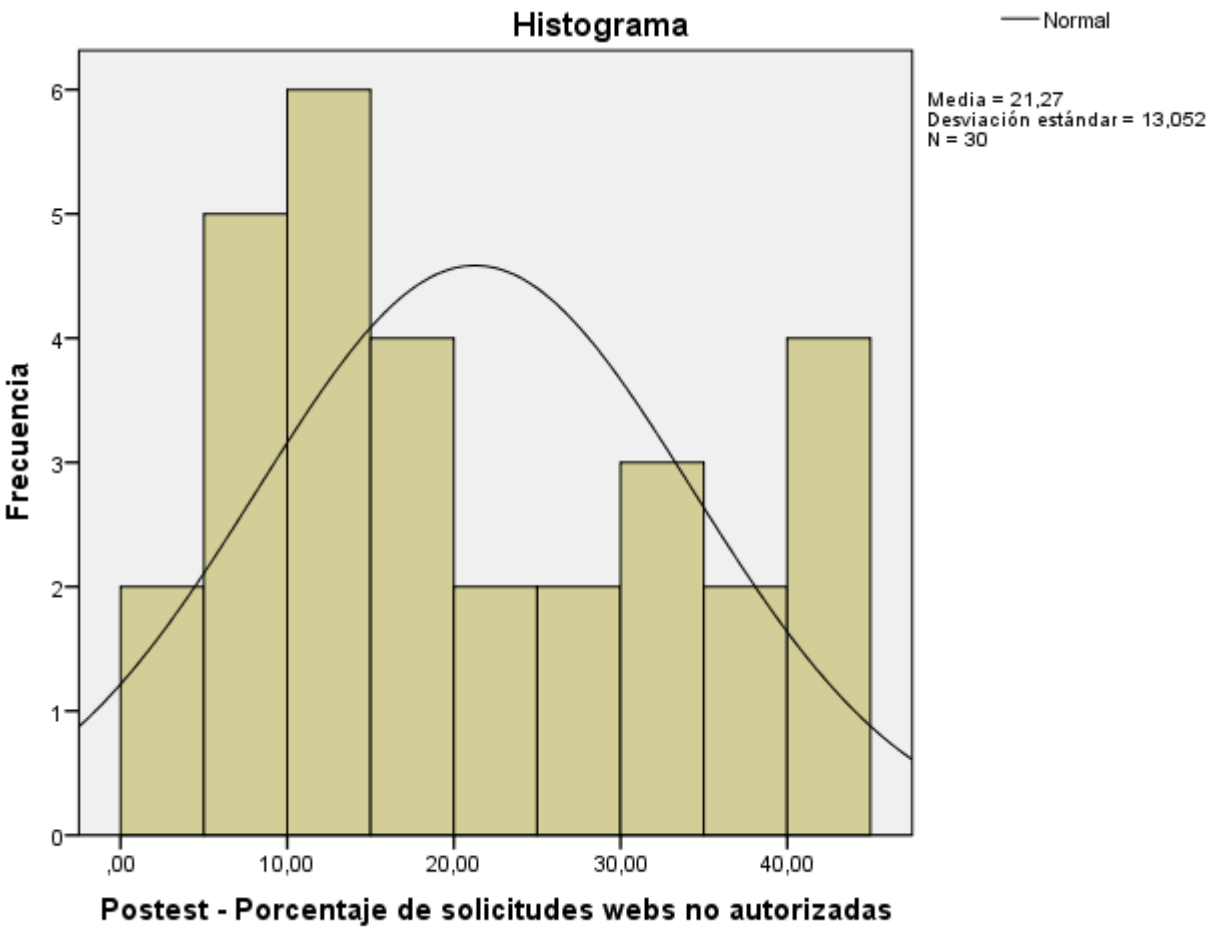
Figura 27: Prueba de Normalidad % de solicitudes web (internet) antes de la implementación del modelo de seguridad



Fuente: SPSS (propio)

En la figura 28, se muestra un histograma de los valores obtenidos por el indicador "% solicitudes web (internet)" después de implementar el modelo de seguridad en el Grupo Suez, obteniendo una media de 21.27 en el valor porcentual. Además, en el eje horizontal los valores de porcentaje de solicitudes web (internet), y en el eje vertical se puede observar el número de veces que se representan los valores porcentuales en un intervalo, es decir, la frecuencia se puede apreciar como las barras no guarda proporción a la curva de distribución normal y esto es debido a que no existe distribución normal.

Figura 28: Prueba de Normalidad % de solicitudes web después de la implementación del modelo de seguridad



Fuente: SPSS (propio)

3.2.2 Prueba de Hipótesis

Como la prueba de normalidad, dio como resultado que los datos de los indicadores "porcentaje de disponibilidad de la información" y "porcentaje de solicitudes webs (internet)" no cumplen el requisito de distribución normal se utilizó la prueba de Wilcoxon para muestras relacionadas. (Ver tablas)

a) Hipótesis de investigación 1

H1: El modelo de seguridad mejorara la disponibilidad de la información, basada en la norma ISO/IEC 27002:2013, en el Grupo SUEZ.

Indicador: Porcentaje de disponibilidad de la información.

Hipótesis Estadística

Definición de variables:

PDIa: % de disponibilidad de la información antes del modelo de seguridad.

PDId: % de disponibilidad de la información después del modelo de seguridad.

H1o: El modelo de seguridad no aumenta el porcentaje de disponibilidad de la información.

H1o: PDId ≤ PDIa

H1a: El modelo de seguridad aumenta el porcentaje de disponibilidad de la información.

H1o: PDId ≥ PDIa

Tabla 8: Diferencia significativa en el porcentaje de disponibilidad de la información antes y después del modelo de seguridad

	Z	Sig. asintótica (bilateral)
Postest Porcentaje de disponibilidad de la información – Pretest Porcentaje de disponibilidad de la información	-4,782[b]	,000

a. Prueba de Willcoxon de los rangos con signos.

b. Se basa en rangos negativos.

Fuente: SPSS (propio)

Los resultados de la prueba de Wilcoxon muestran que el valor de significancia (P) es 0.00 menor a 0.05 lo que significa que existe una diferencia significativa en el porcentaje de disponibilidad de la información antes y luego del uso del modelo de seguridad.

Tabla 9: % disponibilidad de la información antes y después del modelo de seguridad

		N	Rango promedio	Suma de rangos
Postest % de disponibilidad de la información. Pretest % de disponibilidad de la información	Rangos negativos	0[a]	,00	,00
	Rangos positivos	30[b]	15,50	465,00
	Empates	0[c]		
	Total	30		

a. Postest % de disponibilidad de la información < Pretest % de disponibilidad de la información

b. Postest % de disponibilidad de la información > Pretest % de disponibilidad de la información

c. Postest % de disponibilidad de la información = Pretest % de disponibilidad de la información

Fuente: SPSS (propio)

De los resultados logrados en la tabla 10 se concluye que la variable PDId (Porcentaje de disponibilidad de la información después del modelo de seguridad) es mayor que la variable PDIa (Porcentaje de disponibilidad de la información antes del modelo de seguridad), por tanto la hipótesis nula es rechazada y se acepta a la hipótesis alterna.

b) Hipótesis de investigación 2

H2: El modelo de seguridad mejorara las solicitudes web (internet) en el Grupo SUEZ.

Indicador: Porcentaje de solicitudes web.

Hipótesis Estadística

Definición de variables:

PSWa: % de solicitudes web antes de usar el modelo de seguridad.

PSWd: % de solicitudes web luego de usar el modelo de seguridad.

H2o: El modelo de seguridad no mejora las solicitudes web (internet).

$$H2o: PSWd \geq PSWa$$

H1a: El modelo de seguridad mejora las solicitudes web (internet).

$$H2o: PSWd \leq PSWa$$

Tabla 10: Diferencia significativa en el porcentaje de las solicitudes web (internet) antes y después del modelo de seguridad

	Z	Sig. asintótica (bilateral)
Postest - Porcentaje de solicitudes webs no autorizadas - Pretest - Porcentaje de solicitudes webs no autorizadas	-4,782[b]	,000

a. Prueba de Wilcoxon de los rangos con signo

b. Se basa en rangos positivos.

Fuente: SPSS (propio)

Los resultados de la prueba de Wilcoxon muestran que el valor de significancia (P) es 0.00 menor a 0.05 lo que significa que existe una diferencia significativa en el porcentaje de solicitudes web (internet) antes y luego de usar el modelo de seguridad.

Tabla 11: % de solicitudes webs (internet) antes y después del modelo de seguridad

		N	Rango promedio	Suma de rangos
Postest - Porcentaje de solicitudes webs no autorizadas - Pretest - Porcentaje de solicitudes webs no autorizadas	Rangos negativos	30[a]	15,50	465,00
	Rangos positivos	0[b]	,00	,00
	Empates	0[c]		
	Total	30		

a. Postest - Porcentaje de solicitudes webs no autorizadas < Pretest - Porcentaje de solicitudes webs no autorizadas

b. Postest - Porcentaje de solicitudes webs no autorizadas > Pretest - Porcentaje de solicitudes webs no autorizadas

c. Postest - Porcentaje de solicitudes webs no autorizadas = Pretest - Porcentaje de solicitudes webs no autorizadas

Fuente: SPSS (propio)

De los resultados obtenidos en la tabla 12 se puede concluir que la variable PSWd (Porcentaje de solicitudes web (internet) después del modelo de seguridad) es menor que la variable PSWa (Porcentaje de solicitudes web (internet) antes del modelo de seguridad), por tanto la hipótesis nula es rechazada y se acepta a la hipótesis alterna.

IV. DISCUSIÓN

Con los resultados conseguidos en la presente tesis se analizó y se cotejó el "porcentaje de la disponibilidad de la información" y el "porcentaje de solicitudes web (internet)" antes y después de la implementación del modelo de seguridad para el control del tráfico de la red LAN, basado en la ISO/IEC 27002:2013.

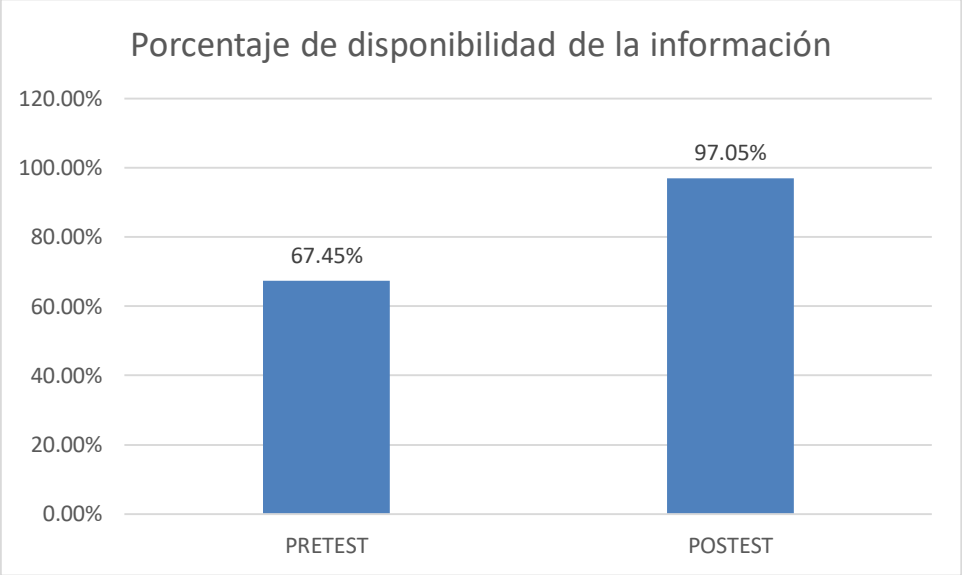
El porcentaje de disponibilidad de la información, en la medición pretest, la media alcanzó 67.45%, y con la implementación del modelo de seguridad la media aumentó a 97,05%. Los resultados conseguidos indican que existe una diferencia positiva de 29.60%. Por tanto, se puede confirmar que la implementación del modelo de seguridad ha logrado aumentar el porcentaje de disponibilidad de la información en el Grupo SUEZ. En ese sentido, tomando como referencia la tesis desarrollada por Bravo Valero (2015) de "modelo diagnóstico y análisis de la red LAN para mejorar el rendimiento y seguridad en la red de salud Valle del Mantaro mediante la metodología Cisco" con respecto al indicador de disponibilidad antes de la implementación del modelo de diagnóstico y análisis fue de 57.02%, y posterior se obtuvo un incremento de 86.05%, el cual se aprecia que también existió una diferencia positiva. Por lo tanto, se puede concluir que los resultados de ambos estudios son similares.

Para el 2do indicador; porcentaje de solicitud de web, en la medición pretest, la media alcanzó 60.21%, y con la implementación del modelo de seguridad la media aumentó a 21,26%. Los resultados obtenidos indican que existe una diferencia positiva de 38.95%. Por tanto, se puede confirmar que la implementación del modelo de seguridad ha logrado recudir la solicitud de acceso a internet, reduciendo el tráfico web hacia internet, y de esta manera mejorando al ancho de banda de la red LAN brindando un mejor canal de ancho de banda para el uso de los aplicativos del Grupo SUEZ. En ese sentido, tomando como referencia la tesis desarrollada por Miranda Torres (2016) de "Implementación de un servidor basado en Linux para la universidad técnica de Cotopaxi" con respecto al indicador de solicitudes web (tráfico hacia internet) concluye que "la implementación de un servidor mejoró notablemente en cuanto al manejo y acceso de los recursos que conforman la red del Laboratorio de Desarrollo de Software, minimizando fallos o caídas en las conexiones y mejorando el rendimiento". Por lo tanto, se puede concluir que los resultados de ambos estudios son similares.

V. CONCLUSIÓN

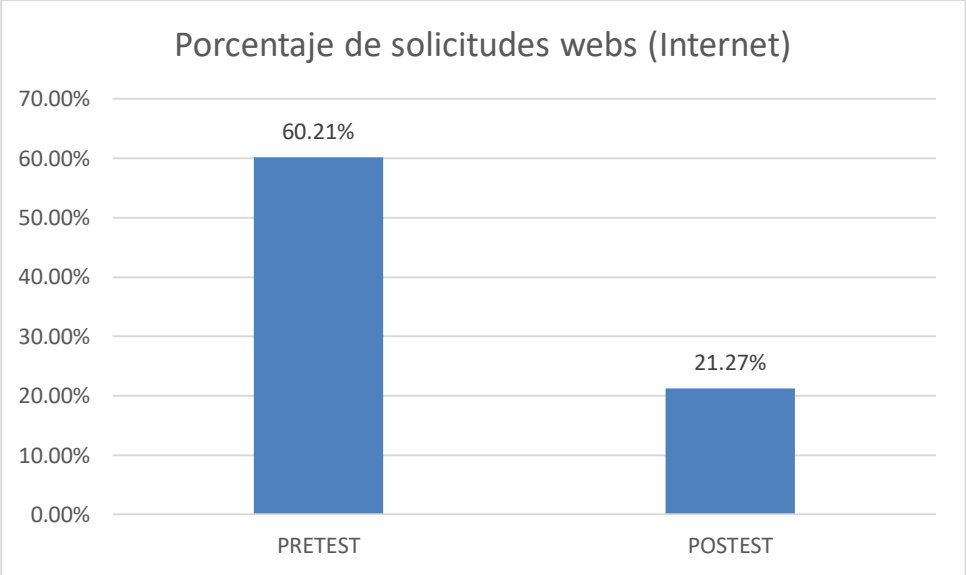
Las conclusiones de la investigación fueron las siguientes:

1. Se ha determinado que el porcentaje de disponibilidad de la información utilizando el modelo de seguridad que controle del tráfico en la red LAN (red de área local) en el Grupo SUEZ aumentó, al no utilizar el modelo de seguridad la media fue de 67,45%, y utilizando el modelo de seguridad la media fue de 97,05%, logrando un incremento de 29,6% que representa mayor flujo y disponibilidad de la información en las cuatro (04) áreas del grupo SUEZ para dar continuidad a los procesos de negocio del Grupo SUEZ.



Fuente: Elaboración Propio (SPSS)

2. Se ha determinado que el porcentaje de solicitudes web (internet) en el Grupo SUEZ utilizando el modelo de seguridad disminuyo, sin el modelo de seguridad la media fue de 60,21%, y utilizando el modelo de seguridad la media fue de 21,26%, esto representa un reducción del 38,95% solicitudes a páginas web (internet) con contenido de entretenimiento y ocio. Asimismo, como efecto mejora el acceso a páginas web productivas y rendimiento del ancho de banda de la red. Por lo tanto, el modelo de seguridad ayudo a optimizar la eficiencia de los aplicativos CONCAR (Sistema de contabilidad) y STARSOFT (Sistema de planillas), de esta manera mejorando los procesos de negocio del Grupo SUEZ obteniendo una percepción positiva de los clientes.



Fuente: Elaboración Propio (SPSS)

VI. RECOMENDACIONES

Recomendaciones con respecto al sistema.

En la presente investigación con título, “Modelo de Seguridad para el Control del Tráfico de la Red LAN, basado en la ISO/IEC 27002:2013 en Grupo SUEZ”, el propósito es el desarrollo de un sistema (aplicativo) que controle la salida (hacia internet) del tráfico de red de la empresa, el mismo que tiene las funcionalidades siguientes:

- Visualización desde un dashboard el tráfico de red tanto de entrada como salida. (Foto de tráfico de input y output).
- Filtrado del contenido de páginas inapropiadas que la empresa considere ser bloqueados, en esta investigación se ha bloqueado las páginas de contenido adultos, youtube y redes sociales.
- Visualización del consumo de ancho de banda, y la generación de reportes de usuarios top con mayor consumo, páginas web con mayores visitas, esta información permitirá la toma de decisiones.

Por lo tanto, las recomendaciones con respecto al sistema es que se adicione los módulos de firewall y Sistema de prevención de intrusos (IPS), ya que estos módulos se complementarían sin mayor dificultad, y sería un sistema de seguridad integral. Que se tome esta investigación como inicio para otras tesis para adicionar mayores funcionalidades, considerando una mayor capacidad de recursos de hardware; como memoria, disco duro y CPU, para lograr un rendimiento alto del sistema de seguridad.

VII. REFERENCIAS

Bibliografía

JIMÉNEZ ALEGRIA, L. C. (2016). Implementación de un sistema de Seguridad (proxy) Open Source basado en Raspberry para Red del Ministerio Público Sede Puno. UCSM.

CABANILLAS CHÁVEZ, J. C. (2015). Propuesta de implementación de control de tráfico de la red con linux para mejorar la calidad de servicio de la red lan en una Universidad privada de la Ciudad de Cajamarca Perú.

VELIZ CASTAÑEDA, J. F. (2016). Aplicación de un firewall con iptables en la empresa Conexion Linux SAC. Universidad Nacional Hermilio Valdizán.

IZQUIERDO CABRERA, J., & TAFUR CALLIRGOS, T. E. (2017). Mecanismos de seguridad para contrarrestar ataques informáticos en servidores web y base de datos. Universidad Señor de Sipán.

PAUCAR FALCÓN, B. H. (2017). Implementación de un Servidor de Seguridad Bajo el S.O GNU/Linux basado en la ISO 27002: 2013 Para mejorar la red de área local del área administrativa del hospital de contingencia Hermilio Valdizán Medrano de Huánuco, 2017. Universidad de Huánuco.

GUEVARA AULESTIA, DAVID OMAR, SÁNCHEZ CUNALATA, DAVID FERNANDO (2017) Implementación de un sistema de monitoreo y protección de datos en la red de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

MOSCOTE MEDINA, RAFAEL LUIS (2017) Sistema de detección y prevención de intrusos ips para la vlan de servidores de la Sociedad Minera de Santander S.A.S. en Bucaramanga (Colombia). 108 P.

ESPINOZA ROMERO, PAÚL FERNANDO (2013) Detección y prevención de intrusos para la protección de los sistemas informáticos en la cooperativa de ahorro y crédito campesina COOPAC.

CEVALLOS MICHILENA, MARIO ANDRES (2013), Metodología de seguridad informática con base en la norma ISO 27002 y en herramientas de prevención de intrusos para la red Administrativa del Gobierno Autónomo Descentralizado de San Miguel de Ibarra. (Ecuador).

BRAVO MORA BRIGGITTE STEPHANIE, DAUDO NIETO ADRIANA ANABEL (2017) Diseño de Gestión de Seguridad de la Información en Base a la Norma ISO 27002 y al estudio de situación actual de la empresa proveedora de internet “POSORJA en acción CIA. LTDA.”

RUIZ OSORIO, DANIEL FERNANDO (2015) Implementación de un esquema de seguridad basado en herramientas Linux para la Cooperativa de Ahorro y Crédito Microempresas de Colombia.

BASE LEGAL (Normas Legales establecido en Perú)

CISCO. (2008). Internetworking Technology Handbook. Recuperado el 01 de junio de 2016,http://www.cisco.com/en/US/docs/internetworking/technology/handbook/ito_doc.html

VALENTINE, M., & WHITAKER, A. (2008). CCNA Exam Cram (Exam 640-802). Pearson IT Certification.

ANDREW L. RUSSELL (2013). OSI: The Internet That Wasn't. How TCP/IP eclipsed the Open Systems Interconnection standards to become the global protocol for computer networking. IEEE Spectrum. Recuperado e: http://spectrum.ieee.org/computing/networks/osithe-internet-that-wasnt

CISCO. (2014, 15 de octubre). CCNA Exploration. Aspectos Básicos de Networkiing. Recuperado de www.netacad.com

CONTRERAS, O Y CONTRERAS. N. (2010). Modelo Matemático para la Predicción de Ancho de Banda. Primera Aproximación. Artículo científico. Subgerencia de Administración y Operación de Redes – Ingeniería. Chile.

HERNÁNDEZ, R., FERNÁNDEZ, C. Y BAPTISTA, M. P. (2014). Metodología de la investigación. McGRAW-HILL / Interamericana Editores, S.A. DE C.V. México.

HERNÁNDEZ, R., FERNÁNDEZ, C. Y BAPTISTA, P. (2006). Metodología de la investigación, C4ta versión, McGraw-Hill interamericana.

ISACA (2012a). "Governance of Enterprise IT (GEIT) Survey" Global Edition, ISACA. Consulta: 25 de Abril de 2013: http://www.isaca.org/GEITSurvey2012

LAUDON, K. Y LAUDON, J. (2012). Sistemas de información gerencial. Duodécima edición. México: Pearson Educación.

VARA, A. (2012) Siete pasos para una tesis exitosa. Un método efectivo para las ciencias empresariales. Instituto de investigación de la facultad de ciencias administrativas y recursos humanos. Universidad de San Martin de Porres. Lima. Manuel electrónico disponible en internet: www.aristidesvara.net, pág. 221, 223.

CISCO SYSTEMS LNC, "Virtual Private LAN Service". http://www. cisco. com/application/pdf/ en/us/guest/tech/tk891/ c1 482/ccmigration_ 09186a00

BARCELO ORDINAS JOSEP M., Y OTROS. (2009). Estructura de redes de computadores. Editorial VOC. Madrid - España.

AREITIO BARTOLÍN JAVIER (2008). Redes de computadoras. Segunda edición. Madrid.

JORGE LUIS CARRANZA LUJAN (2006). Implementación y Configuración de redes.1ªEdición. Editorial Megabyte. Lima. Perú.

MCGRAW HILL, 2001. Redes Virtuales VLANs."(2011).

Diseño de redes, Top Down Design Networking, Cisco, Disponible en: http://www.cisco.com/web/learning/le31/le46/cln/qlm/CCDA/design/top-down-approach-to-network-design-3/player.html. Accesado el: [02 febrero 2015]

CHICAIZA IZA, OSCAR (2007). Análisis y Diseño técnico económico de la Red de Interconexión de las redes en el Campus Girón, Sur, Kennedy y Cayambe de la Universidad Politécnica Salesiana sede Quito. Quito.Disponible en: http://dspace.ups.edu.ec/handle/123456789/1685 Accesado el: [3 de Diciembre del 2014]

MARIA AUXILIADORA DESIDERIO RODRIGO. Análisis, Diseño Y Optimización De Una Red Local Con Intervlans Troncalizadas Y Seguridad De Acceso Mediante La Aplicación De Acls. Disponible: http://www.dspace.espol.edu.ec/handle/123456789/323 Accesado el: [28 de Diciembre del 2014]

Network Infrastructure Cisco Systems. Disponible: http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/4x/42nstrct.html

GRIERA, JORDI. 2008. Estructura de Redes de Computadoras. Barcelona : UOC, 2008. págs. 978-84-9788-791-5. ISBN:.

HERERRA, ENRIQUE. 2012. Tecnologías y Redes. Mexico : Limusa, 2012. ISBN: 968-18-6383-6.

KATZ, MATÍAS. 2013. Redes y Seguridad. Mexico : Alfaomega, 2013. pág. 2. ISBN 978-987-1609-28-4.

KUROSE, JAMES F Y KEITH, ROSS W. 2010. Redes de Computadores: Un enfoque descendente. Madrid : Pearson, 2010. 978-84-7829-119-9.

MOLINA, FRANCISCO. 2013. Implantación de los elementos de la Red Local. Bogotá : StarBook, 2013. ISBN: 978-958-762-090-0.

MORO, VALLINA, MIGUEL. 2013. Infraestructura de Redes de Datos y sistemas de telefonia. Madrid : Paraninfo, 2013. 978-84-9732-874-6.

ROMERO, MARIA DEL CARMEN. 2009. Redes Locales. Madrid : Paraninfo, 2009. ISBN: 978-84-9732-764-0.

VALENCIA, FRANCISCO. 2011. Manual Básico de Configuración de Redes Cisco. Madrid : CISCO System, 2011. ISBN: 978-1-14092-938804.

VICTORIA BEMBIBRE. (05 de 01 de 2009). broadcast.p. Obtenido de https://www.definicionabc.com/tecnologia/broadcast.p

HITOSHI KUME. (2002, 243p)Herramientas estadísticas básicas para el mejoramiento de la calidad. Bogotá, Editorial Norma. ISBN 958-04-6719-6

ECURED.CU. (9 DE 2017). Software_libre. Obtenido de https://www.ecured.cu/Software_libre

VIII. ANEXOS

Anexo 01: Indicador 1

FICHA DE OBSERVACION	
Observador	Janter Edison Salazar Mateo
Compañía de estudio	Grupo SUEZ
Empresa	Av. República de Panamá 3490, San Isidro 15047
Indicador utilizado	Porcentaje de disponibilidad de la información
Periodo de observación (Pre-test)	01-09-2018 al 30-09-2018
Periodo de observación (Post- test)	01-10-2018 al 30-10-2018

	PRE - TEST		POST - TEST	
Reportes	Cantidad de tickets	% Disponibilidad de la información	Cantidad de tickets	% Disponibilidad de la información
1	290	79.93%	10	99.38%
2	650	54.93%	24	98.40%
3	450	68.82%	30	97.99%
4	370	74.38%	60	95.90%
5	680	52.85%	5	99.72%
6	370	74.38%	20	98.68%
7	350	75.76%	80	94.51%
8	650	54.93%	30	97.99%
9	310	78.54%	52	96.46%
10	740	48.68%	77	94.72%
11	500	65.35%	64	95.63%
12	280	80.63%	90	93.82%
13	320	77.85%	8	99.51%
14	680	52.85%	15	99.03%
15	370	74.38%	17	98.89%
16	350	75.76%	26	98.26%
17	650	54.93%	37	97.50%
18	310	78.54%	42	97.15%
19	680	52.85%	53	96.39%
20	370	74.38%	91	93.75%
21	350	75.76%	76	94.79%
22	650	54.93%	14	99.10%
23	310	78.54%	32	97.85%
24	500	65.35%	41	97.22%
25	280	80.63%	28	98.13%
26	320	77.85%	32	97.85%
27	800	44.51%	47	96.81%
28	652	54.79%	83	94.31%
29	378	73.82%	76	94.79%
30	480	66.74%	43	97.08%

Anexo 02: Indicador 2

FICHA DE OBSERVACION	
Observador	Janter Edison Salazar Mateo
Compañía de estudio	Grupo SUEZ
Empresa	Av. República de Panamá 3490, San Isidro 15047
Indicador utilizado	Porcentaje de satisfacción de usuario
Periodo de observación (Pre-test)	01-09-2018 al 30-09-2018
Periodo de observación (Post- test)	01-10-2018 al 30-10-2018

	PRE - TEST			POST - TEST		
Reportes	N° de solicitudes webs no autorizadas	Total de solicitudes webs	% de solicitudes webs (internet)	Cantidad de solicitudes webs (internet)	Total de solicitudes webs	% de solicitudes webs (internet)
1	421	800	52.63%	200	821	24.36%
2	524	750	69.87%	210	767	27.38%
3	614	950	64.63%	410	989	41.46%
4	328	570	57.54%	250	577	43.33%
5	421	680	61.91%	210	715	29.37%
6	415	970	42.78%	170	993	17.12%
7	428	650	65.85%	280	721	38.83%
8	424	650	65.23%	320	845	37.87%
9	519	859	60.42%	280	912	30.70%
10	422	740	57.03%	192	879	21.84%
11	321	500	64.20%	217	621	34.94%
12	618	987	62.61%	97	987	9.83%
13	336	520	64.62%	107	536	19.96%
14	324	680	47.65%	307	690	44.49%
15	717	1200	59.75%	147	1225	12.00%
16	426	865	49.25%	107	884	12.10%
17	338	650	52.00%	67	672	9.97%
18	215	417	51.56%	177	436	40.60%
19	429	680	63.09%	217	695	31.22%
20	556	970	57.32%	177	980	18.06%
21	641	817	78.46%	121	836	14.47%
22	628	921	68.19%	113	927	12.19%
23	614	928	66.16%	98	942	10.40%
24	421	649	64.87%	74	664	11.14%
25	302	621	48.63%	98	634	15.46%
26	714	928	76.94%	72	932	7.73%
27	742	985	75.33%	80	992	8.06%
28	624	1025	60.88%	60	1036	5.79%
29	421	853	49.36%	40	872	4.59%
30	342	718	47.63%	20	741	2.70%

UCV Universidad César Vallejo	ACTA DE APROBACIÓN DE ORIGINALIDAD DE TESIS	Código : F06-PP-PR-02.02 Versión : 07 Fecha : 23-03-2018 Página : 1 de 1

Yo, **MANUEL HILARIO FALCON**, docente de la Facultad INGENIERIA y Escuela Profesional INGENIERIA DE SISTEMAS de la Universidad César Vallejo LIMA ESTE - SJL, revisor (a) de la tesis titulada:

"MODELO DE SEGURIDAD PARA EL CONTROL DEL TRÁFICO DE LA RED LAN, BASADO EN LA ISO/IEC 27002:2013 EN GRUPO SUEZ", del estudiante JANTER EDISON SALAZAR MATEO, constato que la investigación tiene un índice de similitud de 25 % verificable en el reporte de originalidad del programa Turnitin.

El/la suscrito (a) analizó dicho reporte y concluyó que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

Lima, San Juan de Lurigancho 11 de diciembre del 2018

.....

MANUEL HILARIO FALCON

DNI: 10132075

Elaboró	Dirección de Investigación	Revisó	Secretaría de Investigación	Aprobó	Vicerrectorado de Investigación

UCV UNIVERSIDAD CÉSAR VALLEJO	AUTORIZACIÓN DE PUBLICACIÓN DE TESIS EN REPOSITORIO INSTITUCIONAL UCV	Código : F08-PP-PR-02.02 Versión : 09 Fecha : 23-03-2018 Página : 1 de 1

Yo **SALAZAR MATEO JANTER EDISON**, identificado con DNI N° **42545103**, egresado(a) de la Carrera Profesional de Ingeniería Sistemas de la Universidad César Vallejo, autorizo (**X**), no autorizo ( ) la divulgación y comunicación pública de mi trabajo de investigación titulado " **MODELO DE SEGURIDAD PARA EL CONTROL DEL TRAFICO DE LA RED LAN, BASADO EN LA ISO/IEC 27002:2013 EN GRUPO SUEZ**" en el Repositorio Institucional de la UCV (http://repositorio.ucv.edu.pe/), según lo estipulado en el Decreto Legislativo 822, Ley sobre Derecho de Autor, Art. 23 y Art. 33

Fundamentación en caso de no autorización:

.....
.....
.....
.....
.....
.....
.....
.....

SALAZAR MATEO JANTER EDISON

DNI: **42545103**

Fecha: 14 de Diciembre del 2018

Firma	Dirección de Investigación	Firma			

UNIVERSIDAD CÉSAR VALLEJO

AUTORIZACIÓN DE LA VERSIÓN FINAL DEL TRABAJO DE INVESTIGACIÓN

CONSTE POR EL PRESENTE EL VISTO BUENO QUE OTORGA EL ENCARGADO DE INVESTIGACIÓN DE Mg. ACUÑA MELENDEZ MARIA EUDELIA.

A LA VERSIÓN FINAL DEL TRABAJO DE INVESTIGACIÓN QUE PRESENTA EL ALUMNO **SALAZAR MATEO JANTER EDISON**, ESTA APTO PARA ENTREGAR LA TESIS DIGITAL A LA BIBLIOTECA.

INFORME TÍTULADO:

"MODELO DE SEGURIDAD PARA EL CONTROL DEL TRAFICO DE LA RED LAN, BASADO EN LA ISO/IEC 27002:2013 EN GRUPO SUEZ"

PARA OBTENER EL TÍTULO O GRADO DE: **INGENIERO DE SISTEMAS**

SUSTENTADO EN FECHA: **11 DE DICIEMBRE DEL 2018**

NOTA O MENCIÓN: **14 (CATORCE).**

ACUÑA MELENDEZ MARIA EUDELIA

Reporte de Turnitin al 25% de coincidencias